U.S. Department of Justice

National Security Division

Office of the Assistant Attorney General *Washington, D.C. 20530*

April 20, 2007

MEMORANDUM

TO: Honorable Roger Vinson, Judge
U.S. Foreign Intelligence Surveillance Court

FROM: Kenneth L. Wainstein Ken Wainstein / MCD

SUBJECT: Report in No. [redacted]

On March 21, 2007, the Government filed an application, Docket No. [redacted] under the electronic surveillance provisions of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-1811, seeking renewal of the surveillance authority for the National Security Agency granted in Docket No. [redacted] Like the application in No. [redacted] this application identified the "target" of the proposed surveillance as [redacted] foreign powers: [redacted] The application identified the "facilities" at which the surveillance was to be directed [redacted] It also proposed minimization procedures that would have required the Government to report to the Court every 30 days concerning new telephone numbers and e-mail addresses used by NSA as foreign selectors. It did not require the Court make probable cause determinations with respect to individual existing or new foreign selectors. ~~(TS//SI//NF)~~

On March 29, you advised us that you had reservations about the legal theory advanced in the Government's application. You then issued an Order and Memorandum Opinion setting forth your reasoning on April 3. In your Opinion, you did not take issue with our identification of the targets of the proposed electronic surveillance as the [redacted] foreign powers noted above. But you concluded that the facilities at which the surveillance is directed are the individual telephone numbers and e-mail addresses used by NSA as selectors and found the application inadequate under FISA because it did not provide a probable cause justification for each selector. In addition, you expressed concern that our proposed reporting procedure was contrary to the language of FISA in that it provided for after-the-fact reporting rather than prior judicial authorization. Thus, you found that our proposed minimization procedures did not meet the definition of such procedures under section 1801(h).

Understanding our need for time to address your concerns, you allowed us to seek—and we obtained—an extension of the authorization granted in No. [redacted] until 5 p.m. on May 31, 2007. You instructed us to "periodically submit written reports . . . regarding [our] efforts to prepare and submit for [your] consideration a revised and supplemented application that would

meet the requirements of FISA as described in [your] order and opinion." This memorandum constitutes the first such report, which is due on or before April 20, and sets forth a new proposal that we have crafted to address the concerns you expressed in your Opinion and in our meetings. ~~(TS//SI//NF)~~

New Approach: After-acquired/Roving Surveillance (U)

Since receiving your Opinion, we have examined FISA closely to determine whether there are alternate approaches, anchored in the clear terms of FISA as interpreted in your Opinion, that would allow the Government the speed and agility needed to serve the same early warning function as the surveillance authorized in No. [redacted] We believe that we have developed such an approach, which is significantly different from the approach contained in our prior submission.

Our proposal has two parts. First, unlike our prior submission, this new approach would require the Court, in considering the application, to make a probable cause finding that each of the [redacted] telephone numbers and e-mail addresses included in the application and currently targeted for collection under No. [redacted] is being used or is about to be used by [redacted] targets of the surveillance. Second, for numbers and addresses NSA discovers after the Court grants the application, the new approach relies on those provisions of FISA, and Court practice under them, which allow the Court to authorize the Government to initiate surveillance of new facilities (e.g., telephone numbers and e-mail addresses) used by the same target that the Government identifies after the initial authorization. This authority accounts for targets like the foreign powers here that [redacted] When the Government uses this authority, it must comply with a statutory reporting requirement. That provision, which applies when the nature and location of the facilities at which the surveillance is directed is "unknown" at the time of the application, requires the Government to report the new facility and the probable cause supporting the surveillance of it to the Court within ten days. Also unlike the prior approach, this approach will require the Court to make probable cause determinations with respect to each of the new telephone numbers and e-mail addresses at, or before, renewal. Should the Court agree that this approach is consistent with the statute, we will continue to work with NSA to ensure that it can be accomplished in light of the Government's logistical constraints and in a manner consistent with the operational purpose of the surveillance. ~~(TS//SI//NF)~~

Like the application in No. [redacted] this application would seek authority to conduct surveillance of these foreign powers by tasking for collection only telephone numbers and e-mail addresses reasonably believed to be used outside the United States. It recognizes that these powers operate in a multitude of foreign countries, [redacted] to avoid detection. ~~(TS//SI//NF)~~

Proposed Application for After-acquired/Roving Authority (U)

Our proposed application would be structured as follows:

- We would continue to identify the targets of the electronic surveillance as the [redacted] foreign powers noted above. ~~(TS//SI//NF)~~

- We would identify, as your Opinion does, the "facilities . . . at which the electronic surveillance is directed," § 1804(a)(4)(B), as the individual telephone numbers and e-mail addresses that NSA tasks for collection. ~~(TS//SI//NF)~~

- For each of the foreign selectors currently under surveillance, we would submit for the Court's review "a statement of the facts and circumstances relied upon by the [Government] to justify [its] belief that . . . each of the facilities . . . at which the electronic surveillance is directed is being used, or is about to be used, by" [redacted] identified foreign powers. *Id.* You would then review these facts and circumstances for each of the telephone numbers and e-mail addresses to determine whether probable cause exists. *See id.* § 1805(a)(3)(B). ~~(TS//SI//NF)~~

- We have sent attorneys from the National Security Division (NSD) to NSA to help prepare revised and updated probable cause submissions for these [redacted] facilities. NSD attorneys are working side-by-side with NSA professionals. Together, they are working to modify NSA's existing documentation of each justification—which in most cases was initially prepared for NSA's internal use only—for each facility. With guidance from NSD attorneys, NSA is in the process of reviewing each probable cause submission so that the necessary facts can be provided to the Court in one clear and concise statement. A sample of our probable cause submissions is attached as Exhibit A. ~~(TS//SI//NF)~~

- As we did in our prior application, we would submit the facts and circumstances that underlie our conclusion that [redacted] have other telephone numbers and e-mail addresses that are unknown to NSA at the time of the application, that they will acquire new telephone numbers and e-mail addresses during the period of surveillance, [redacted] ~~(TS//SI//NF)~~

Proposed Order Authorizing Surveillance (U)

If you were satisfied that probable cause existed to conduct electronic surveillance of all or a portion of the specified known facilities and that the statutory requirements were otherwise met, you would issue an order authorizing the surveillance, as follows. *See id.* § 1805. (U)

- The Order would specify "the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known." *Id.* § 1805(c)(1)(B). That is, the Order would specify the telephone numbers and e-mail addresses for which the Court had found probable cause. ~~(TS//SI//NF)~~

- The Order would also recognize that there are facilities used by the targeted foreign powers whose "nature and location" is not "known." *See id.* FISA provides for just such

a circumstance. "[W]here the nature and location of each of the facilities or places at which the surveillance will be directed is unknown," FISA requires the Order to direct the Government to "provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility . . . ." *Id.* § 1805(c)(3). Such notice must include "the nature and location of each new facility or place at which the electronic surveillance is directed" and "the facts and circumstances relied upon by the [Government] to justify [its] belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance." *Id.* The Order would direct us to provide the Court with such notice. (TS//SI//NF)

- At renewal, the Court would review the facts and circumstances provided in the notice as to each surveillance and determine whether probable cause exists for each new facility and the new surveillance may continue. The Court could call for earlier review as well. Section 1805(c)(3)(C) provides that the Government may propose new minimization procedures in its notice to account for the new surveillance. The Court could require that such proposed procedures provide for a Court determination of whether probable cause exists for each new facility and thus whether surveillance may continue, without awaiting the renewal application.[1] ~~(TS//SI//NF)~~

Consistency with Prior Practice and the Language of the Statute (U)

This approach builds upon prior FISA practice and is contemplated by the plain language of the statute, both of which evince the Court's power, in the proper case, to authorize the Government to initiate surveillance immediately upon the Government's finding of probable cause in circumstances where it is anticipated that the target will use facilities that are unknown at the time an order is granted authorizing surveillance. As in the case of roving wiretaps in the criminal context, this authorization is critical to the Government's ability to follow the target in real time and to avoid the loss of valuable information. In order to allow for Court oversight of this authority, the statute and the Court require regular reporting after new surveillance has begun. ~~(S)~~

The Court has a long-standing practice of authorizing the Government, without first returning to the Court for prior approval, to conduct surveillance of telephone numbers, e-mail addresses, and vehicles that the Government later learns are being used by the target of the surveillance.

(b)(1); (b)(3); (b)(7)(A)

[redacted]

[1] Alternatively, the Court could authorize the initial surveillance for a period of less than 90 days and review the probable cause underlying the surveillance of the new facilities at that earlier time.

(b)(1); (b)(3); (b)(7)(A)

As noted above, section 1805(c)(1)(B) provides that an Order need not specify the nature or location of facilities that are not "known." *Id.* It thus recognizes the Court's power to authorize surveillance directed at facilities for which the Government learns of probable cause after the initial order. In such circumstances, FISA establishes a reporting mechanism to ensure that the Court can conduct informed oversight of the Government's use of this authority. *See id.* § 1805(c)(3). Although the legislative history of the reporting provision indicates that it was enacted to provide a mechanism for Court oversight of the authority granted by the USA PATRIOT Act in section 1805(c)(2)(B), where the "person" who must provide assistance to the Government is unknown at the time of the order, nothing in the language of the statute restricts it to that context only. Rather, it applies whenever "the nature and location of each of the facilities or places at which the surveillance will be directed is unknown." *Id.* § 1805(c)(3). That is the case here. In order to conduct the surveillance of the specified foreign powers effectively, the Government must be able to add new telephone numbers and e-mail addresses, which are unknown at this time, as they are discovered.[2] ~~(TS//SI//NF)~~

[2] In developing this new approach, we have discovered that prior applications have not read section 1805(c)(3) to require reporting in the traditional after-acquired context, that is, when the Government can identify in the application all of the "specified persons" to whom the secondary orders would be issued. In addition, these applications have read section 1805(c)(3) to apply only when the Government knows neither the "nature" nor the "location" of the new facility or premises. We believe that this reading of the "nature and location" phrase as including two disjunctive requirements both of which must be met is erroneous. The provision uses "is"—the singular form of the verb "to be"—with respect to the term "nature and location." *Id.* § 1805(c)(3). Thus, the term is a unitary concept that refers to whatever identifiers are necessary to specify the facility or place at which the surveillance will be directed. These identifiers will vary according to the type of the facility or place. Because this reporting provision applies whenever the Government does not know the nature and/or location of each of the facilities or places at which the surveillance will be directed, going forward, the Government will follow the

Moreover, this approach is consistent with the language of section 1805(c)(2)(B) and the practice thereunder. This section was amended by the USA PATRIOT Act to allow the Court "in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person" whose assistance is required to effect the surveillance to direct that person to provide such assistance. *See id.*[3] When this provision applies, the identity of the directed person is not contained in the application or Order because it is not known at the time. The Government is then provided with the authority to identify that person and require his assistance without first returning to the Court. Under this provision, the Court has authorized the Government [redacted] within the meaning of section 1805(c)(2)(B). If the target was not the subscriber to the number serviced by the unspecified provider, the FBI in exigent circumstances was authorized to serve a secondary order on the provider for up to 72 hours, after which time the surveillance would have had to have ended unless an OIPR attorney had attested in writing that there was probable cause to believe that the target was using or about to use the [redacted] If the FBI obtained the attestation, the surveillance could continue, subject to a 10-day report to the Court. ~~(TS//SI//NF)~~

We recognize that the authority we seek to conduct this after-acquired/roving surveillance, although founded in both the plain language of FISA and the Court's prior practice, would allow such surveillance on a greater scale than in the past. In addition, the Government would be given broader discretion than in most prior cases to initiate surveillance of a new facility related to the target, that is, the authorization would not be tied to, e.g., [redacted] Our proposal, however, does contain significant safeguards and the discretion required stems from the very reason for this program. The surveillance would be only of the targets' telephone numbers and e-mail addresses reasonably believed to be used outside the United States; the Court would have reviewed the probable cause underlying the surveillance of all initial facilities (which would encompass the large majority of the facilities targeted for collection); the Government would be required to report its probable cause findings for new surveillance to the Court within a short period of time; and the Court would review these findings either at, or before, the time of the subsequent renewal application. In light of the size of this program, the scale of the surveillance authorized under any new approach will be unprecedented. And the Government's discretion to begin surveillance on any new facilities is necessary to any program that will provide the Government the needed flexibility to move rapidly to detect the targets' terrorist plots and to foil their attempts at secrecy and evasion.

---

reporting requirement in all applications that seek authorization to initiate surveillance of facilities or premises discovered after the Court's authorization, regardless of whether this surveillance requires the assistance of a "person" different from the one(s) specified in the order.

[3] This provision does not apply directly in this context. Although the targets here [redacted] the Government will not [redacted] The Government can [redacted] ~~(TS//SI//NF)~~

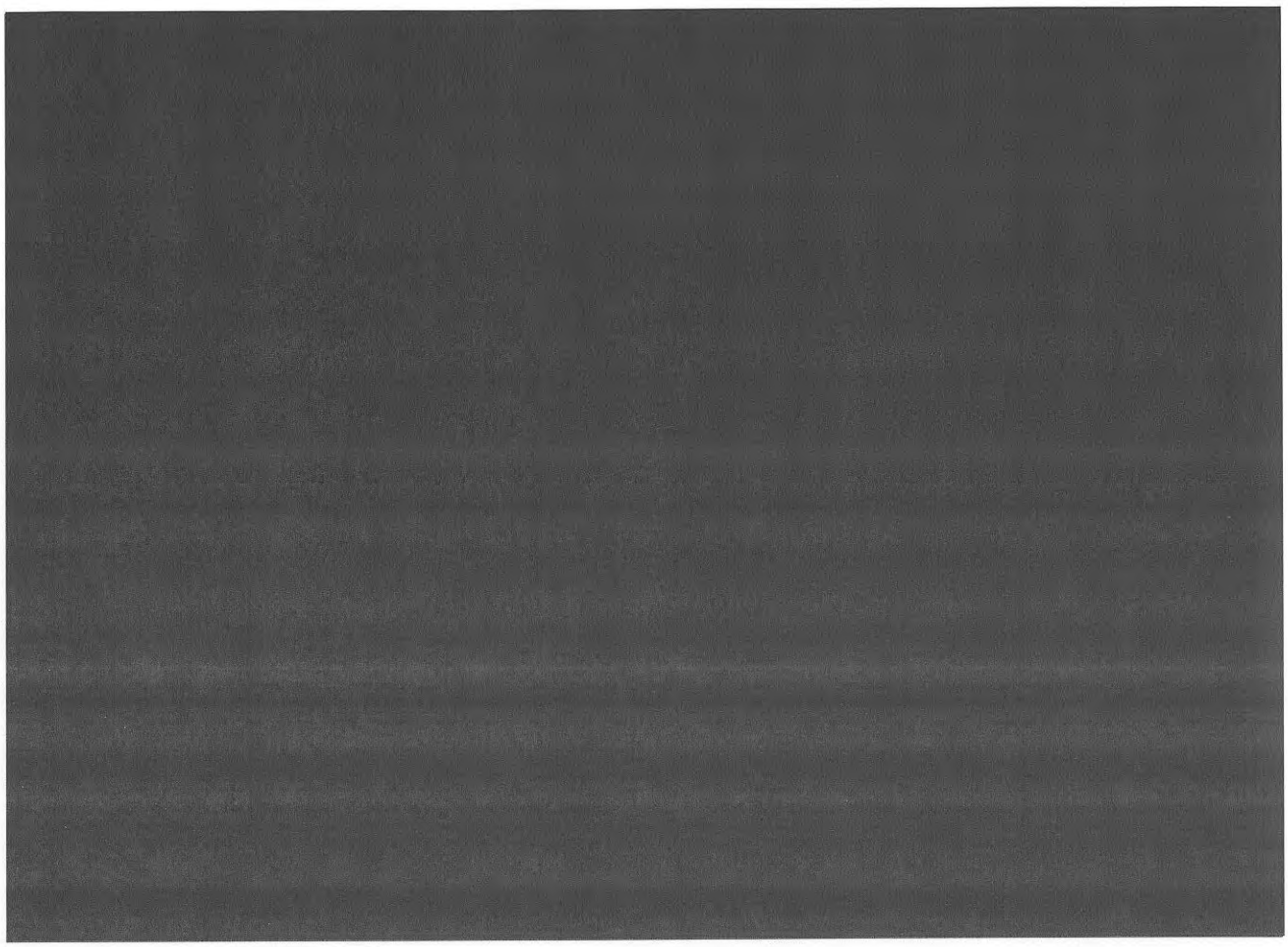
Under our approach, any new surveillance would come under the Court's oversight in a matter of days and it would remain supervised thereafter. (~~TS//SI//NF~~)

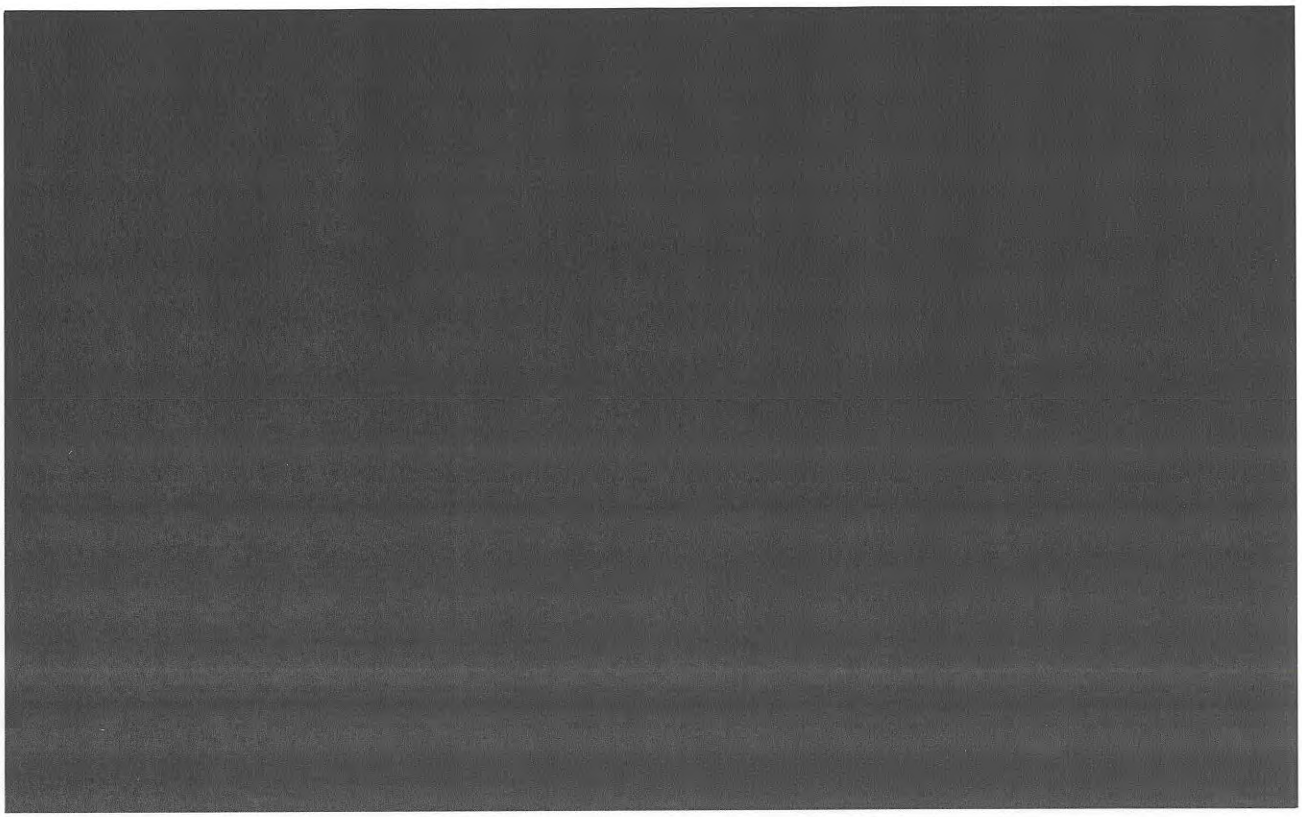
* * *

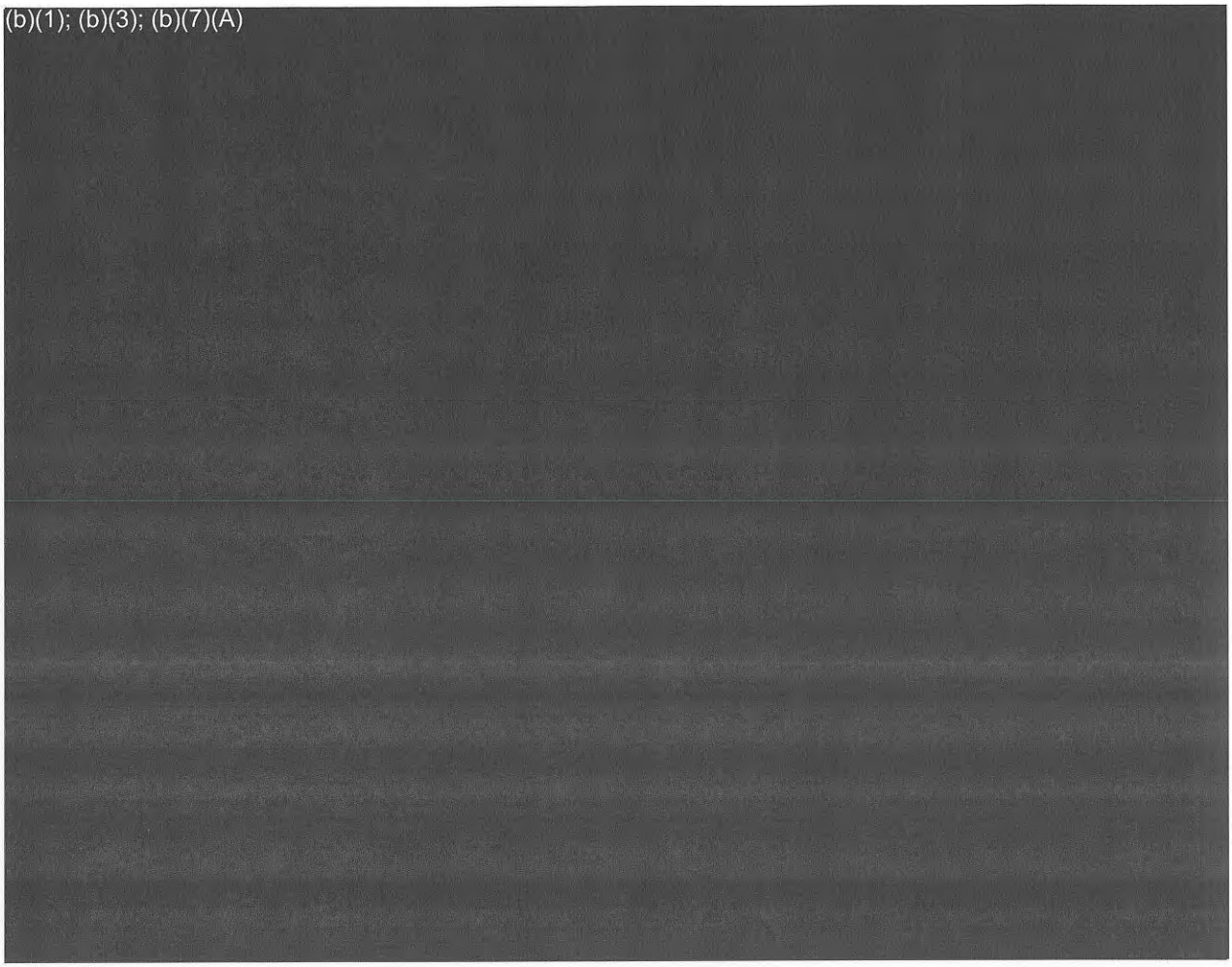
We would like to discuss with you the approach set forth above. We believe that it addresses the concerns you expressed to us, is consistent with FISA and the Court's prior practice, allows the Government the speed and agility it needs to operate this early warning system, and provides for the judicial oversight FISA envisions. We remain committed to developing an approach that satisfies these conditions. Because of the time constraints on pursuing this or other options, we respectfully request that the Court provide us its views on this approach as quickly as possible. (~~TS//SI//NF~~)

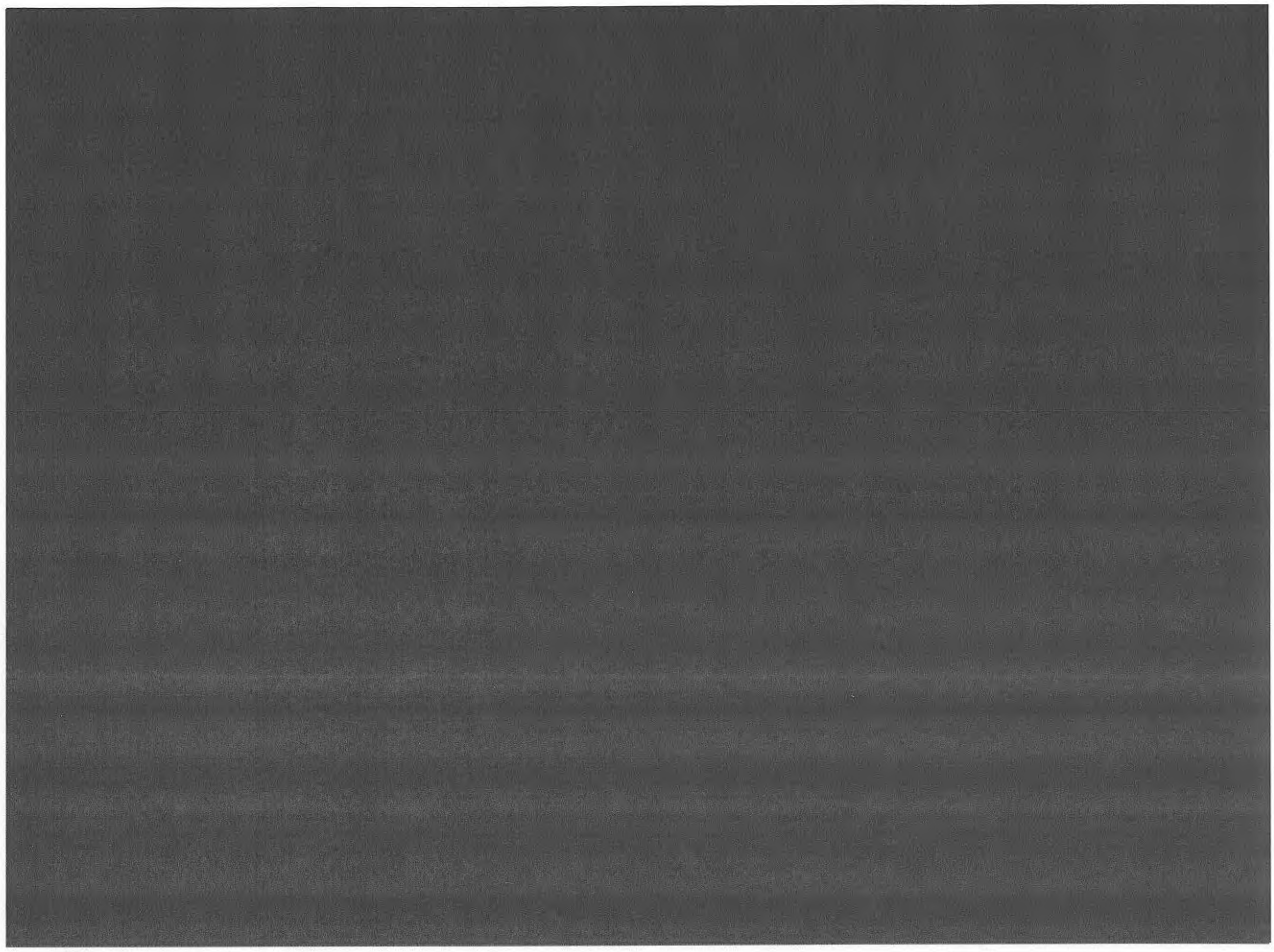
TAB

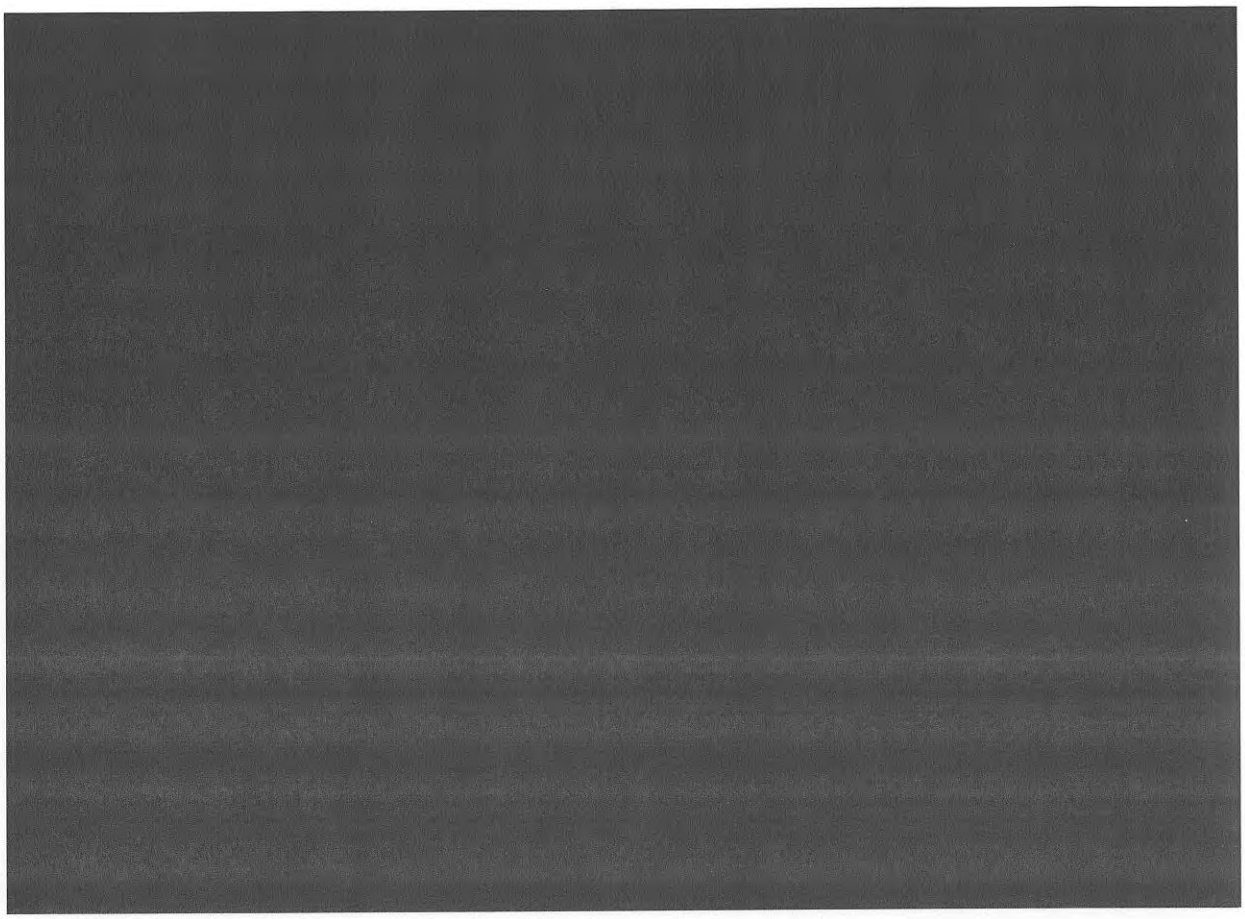
A

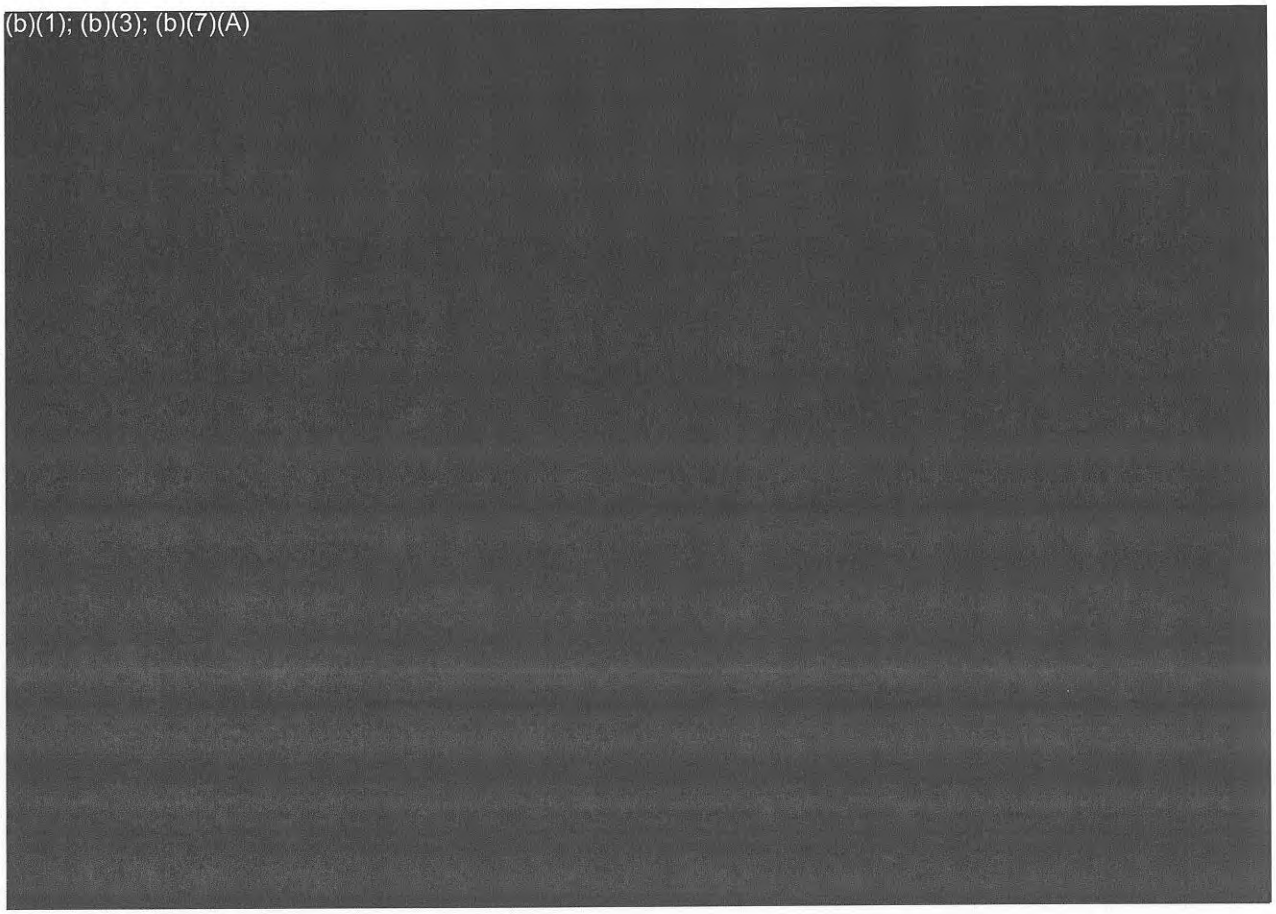


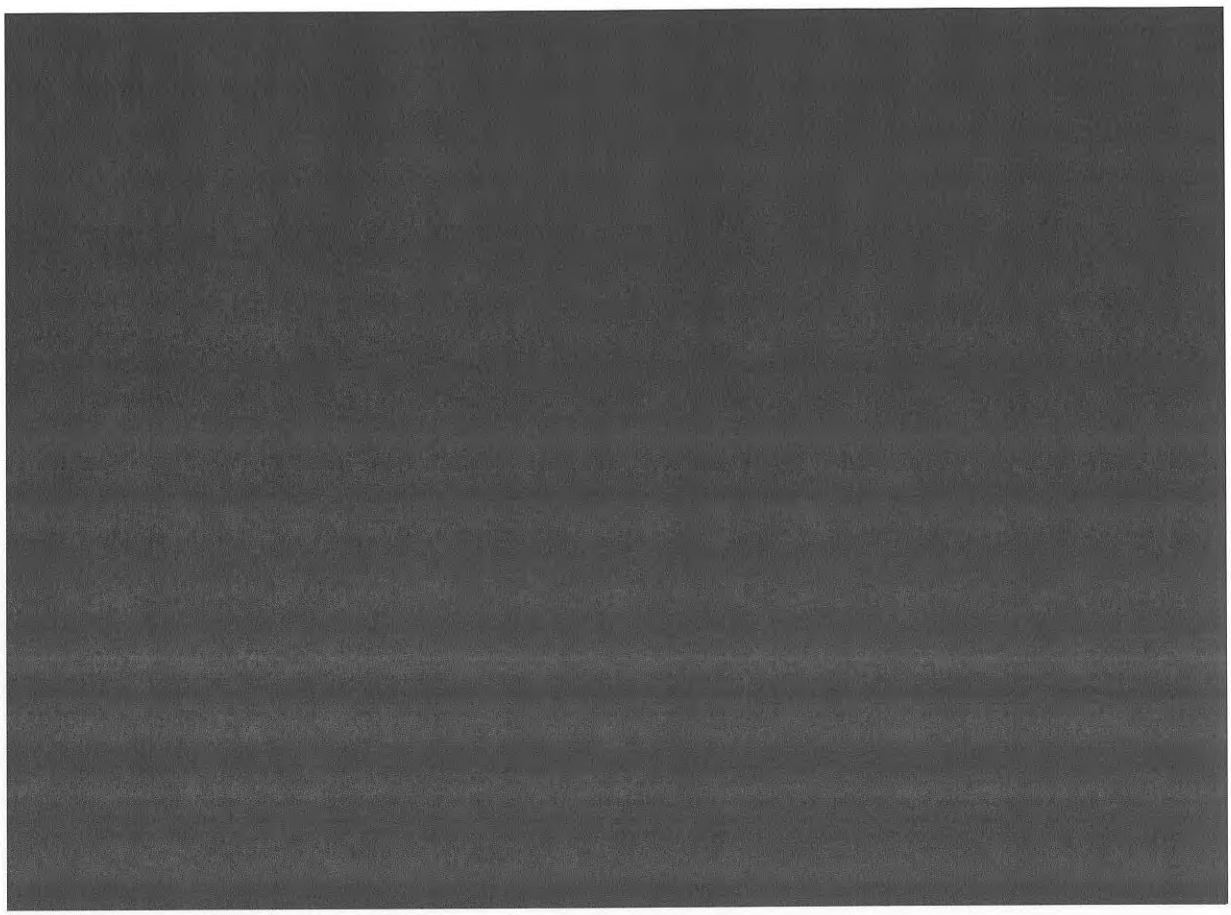


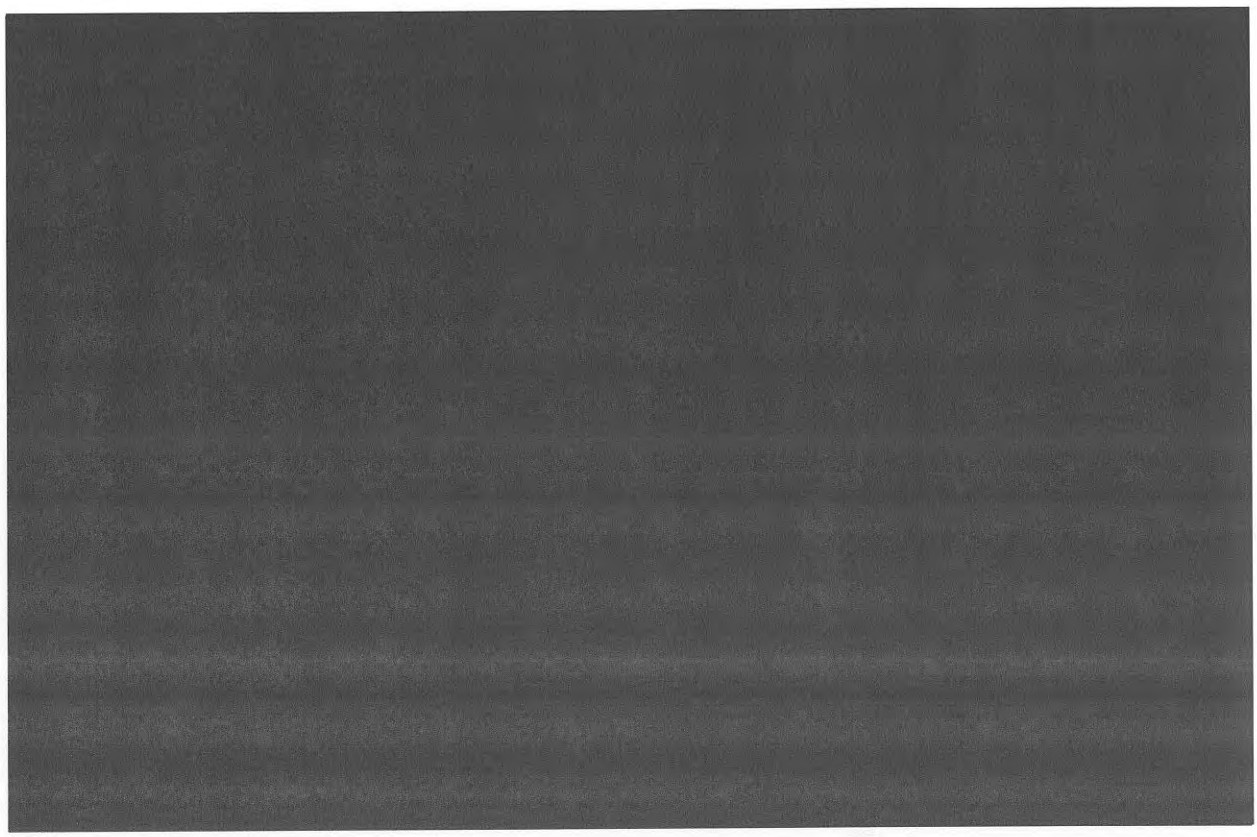


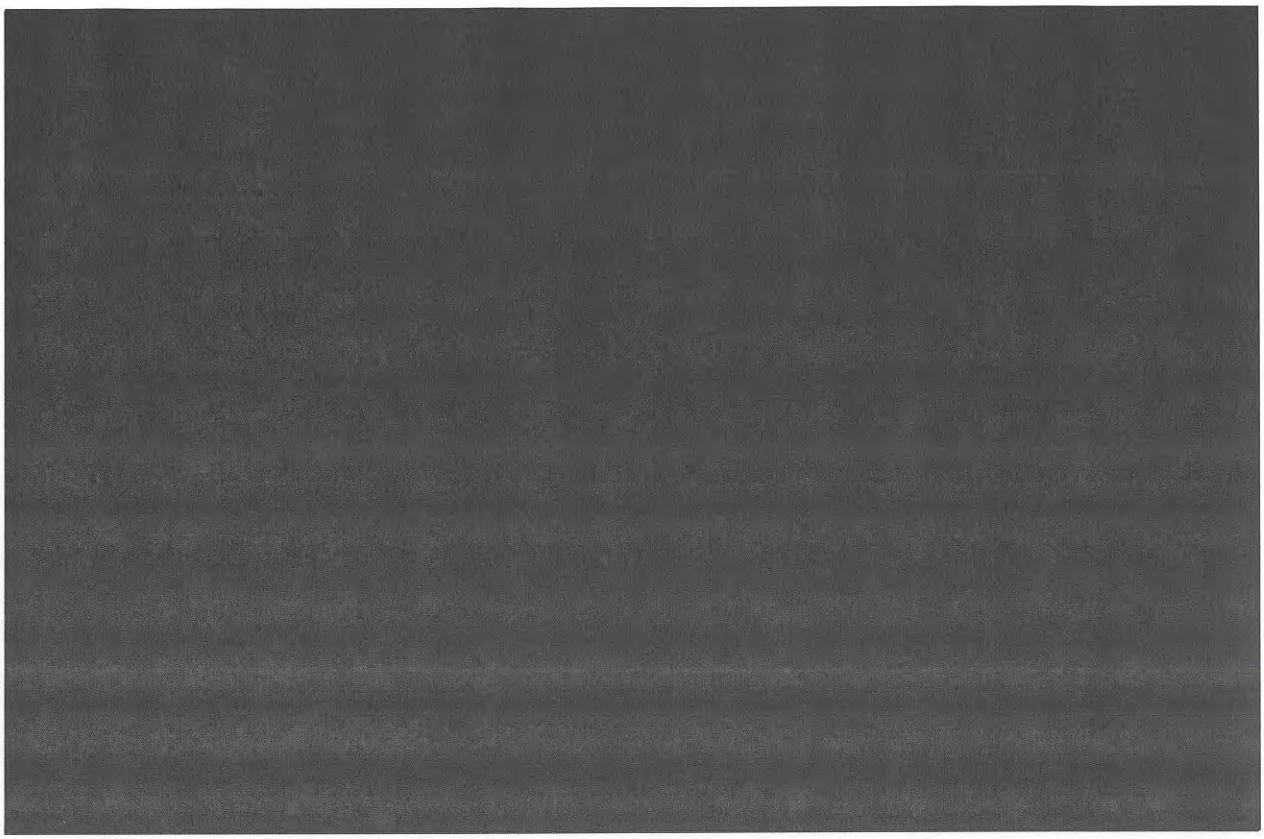


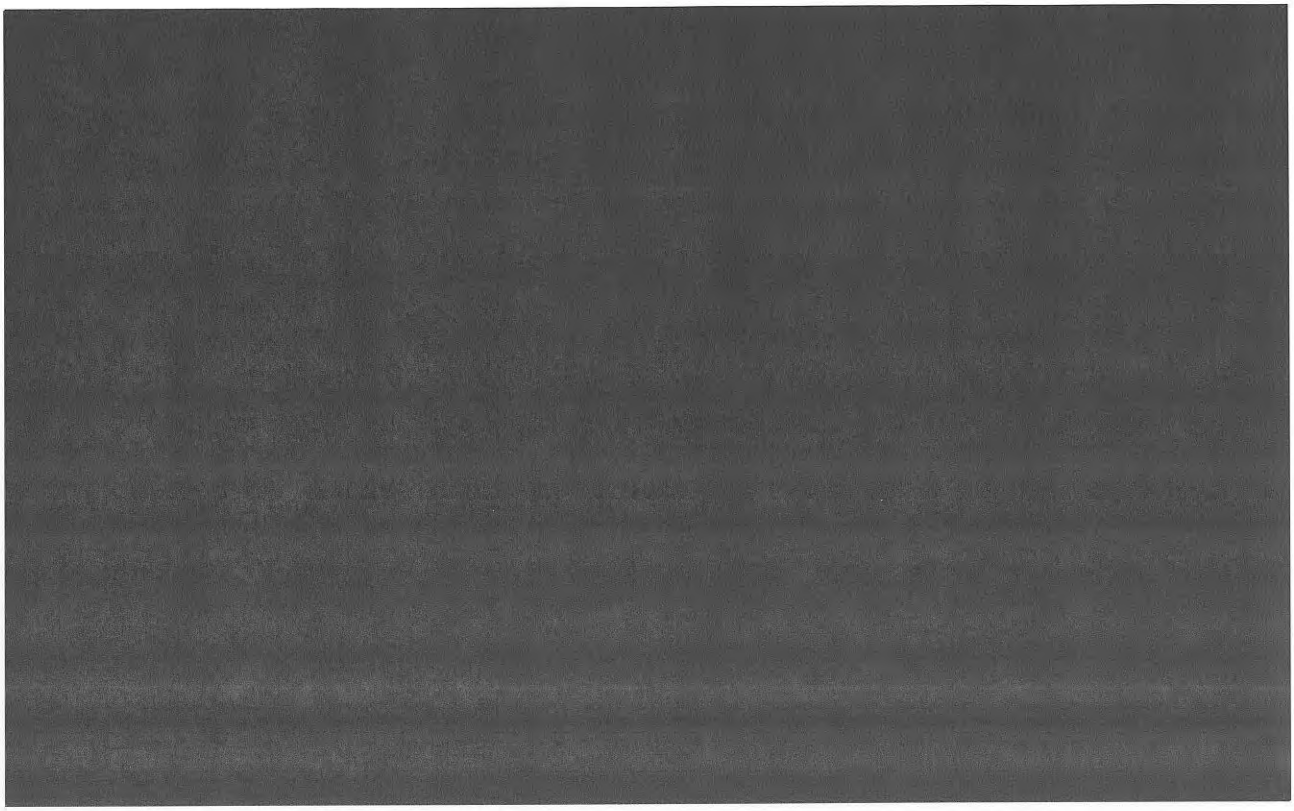


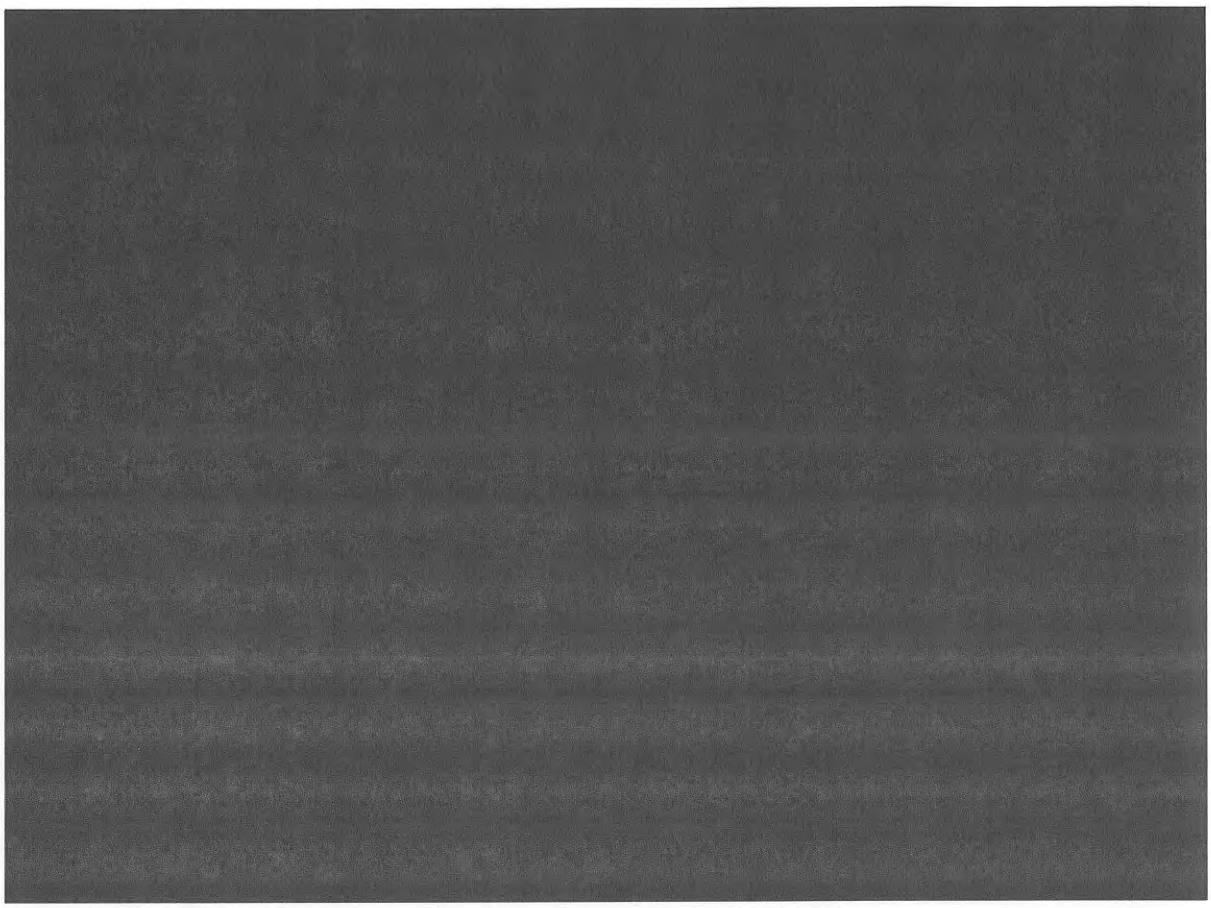


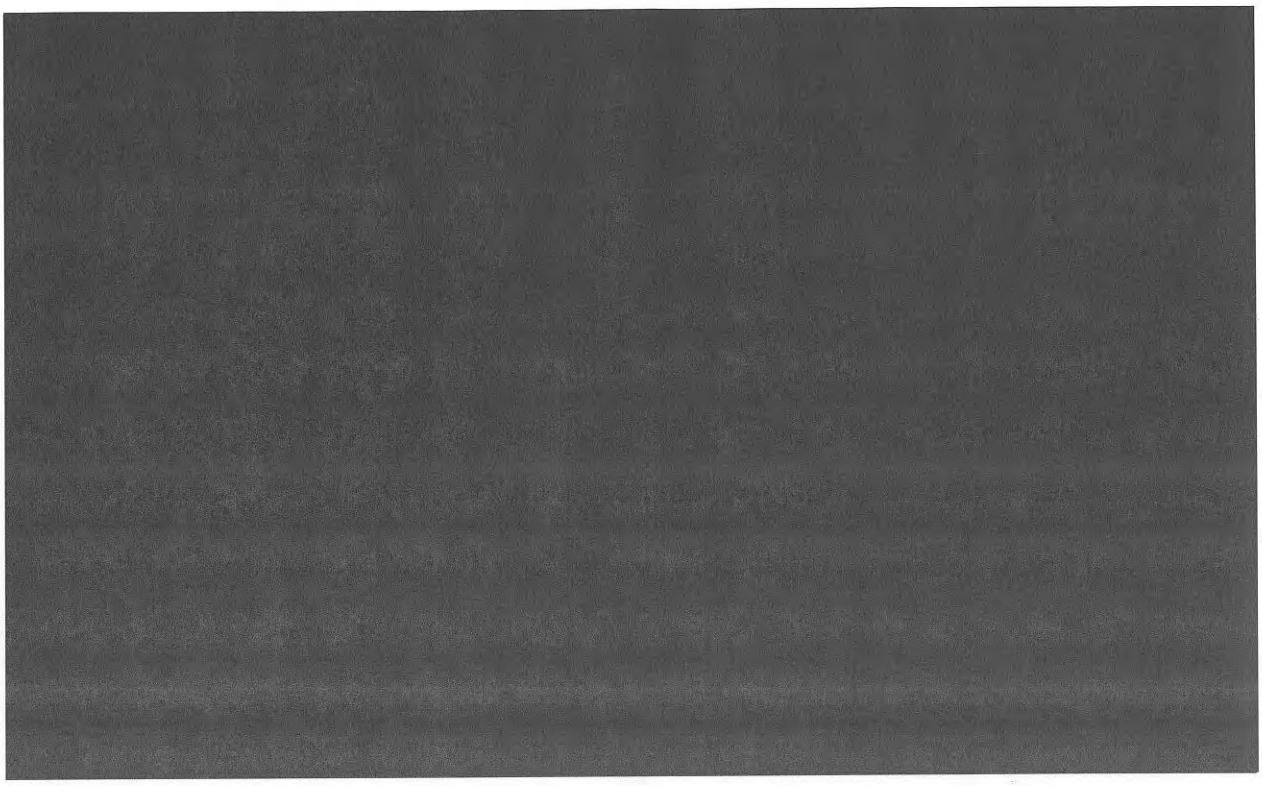


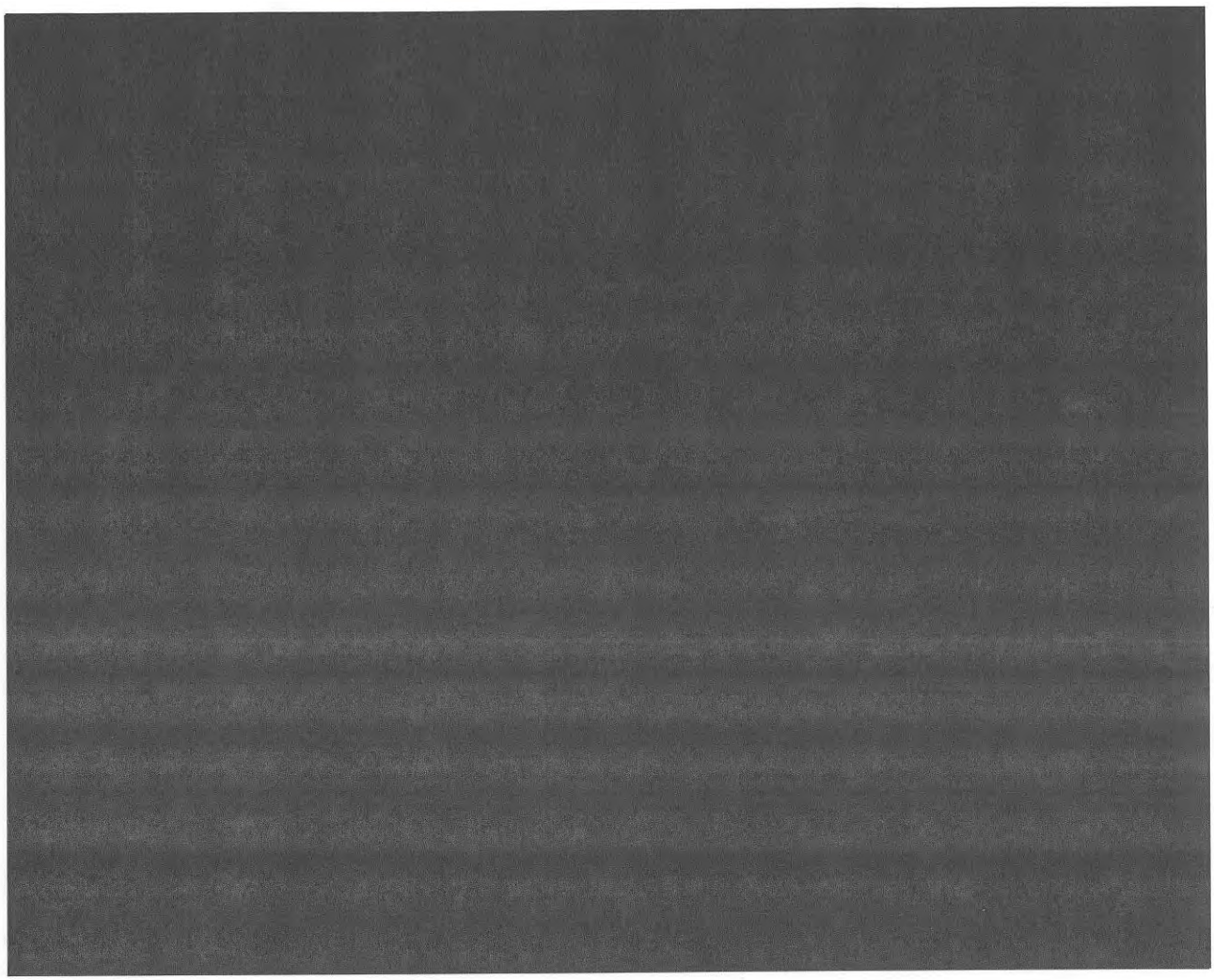


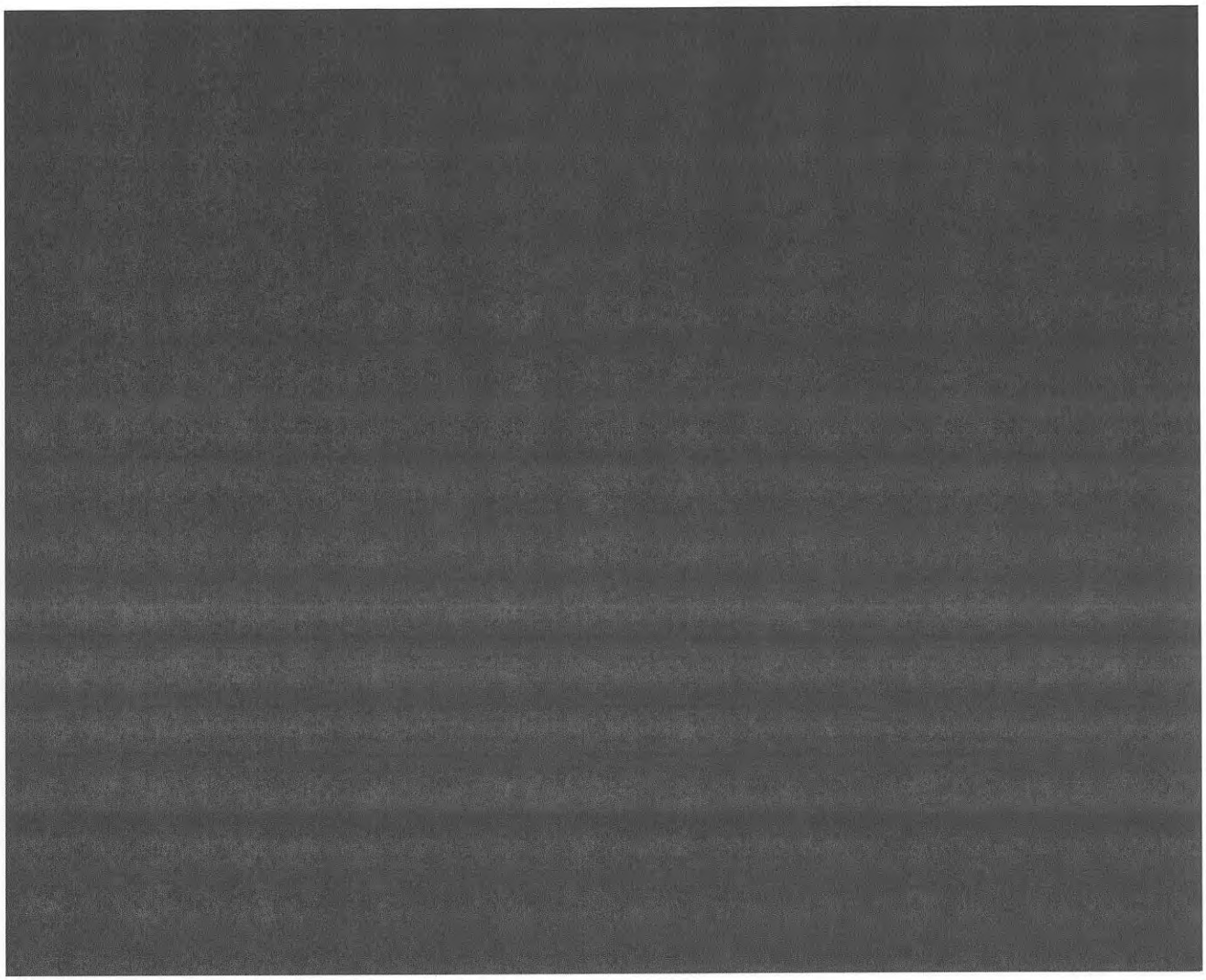


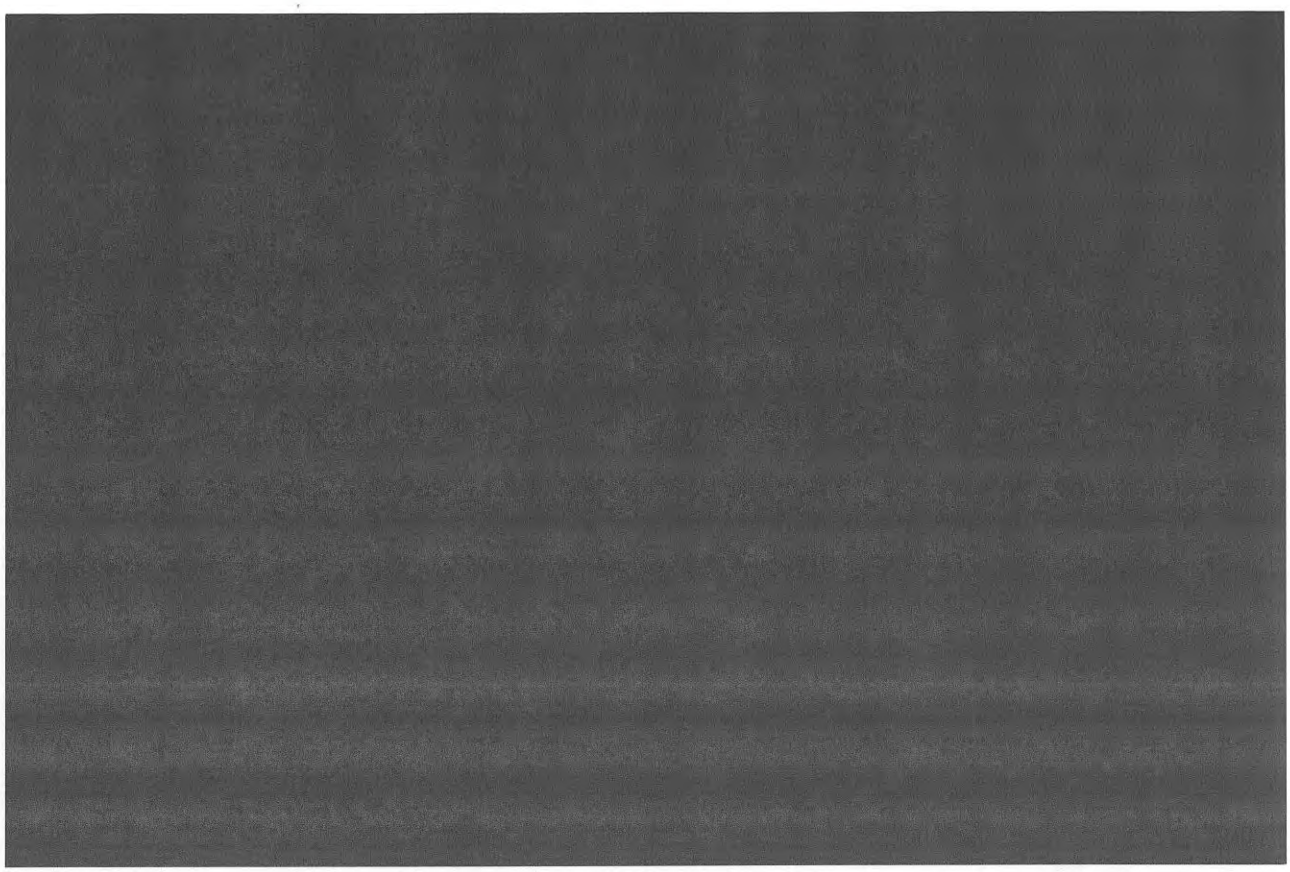


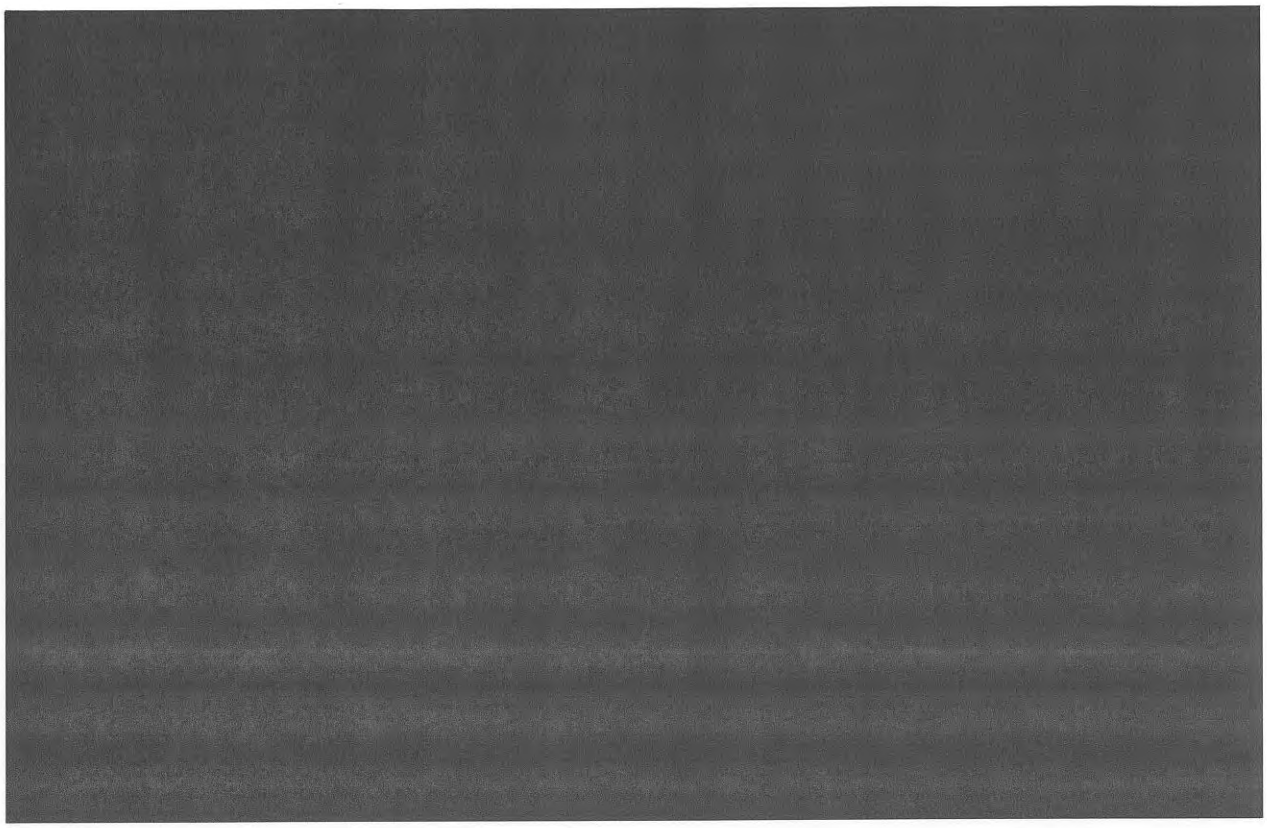


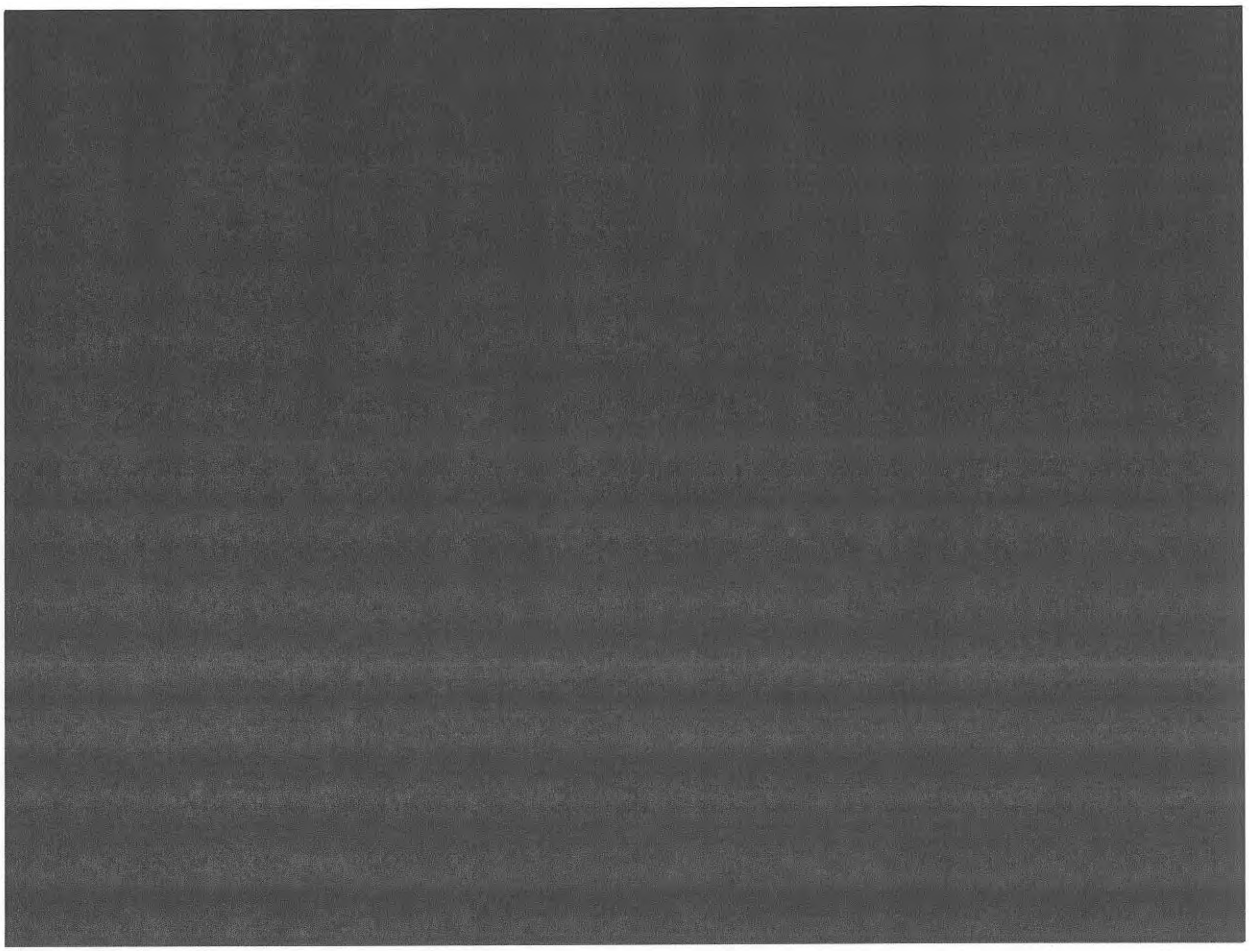


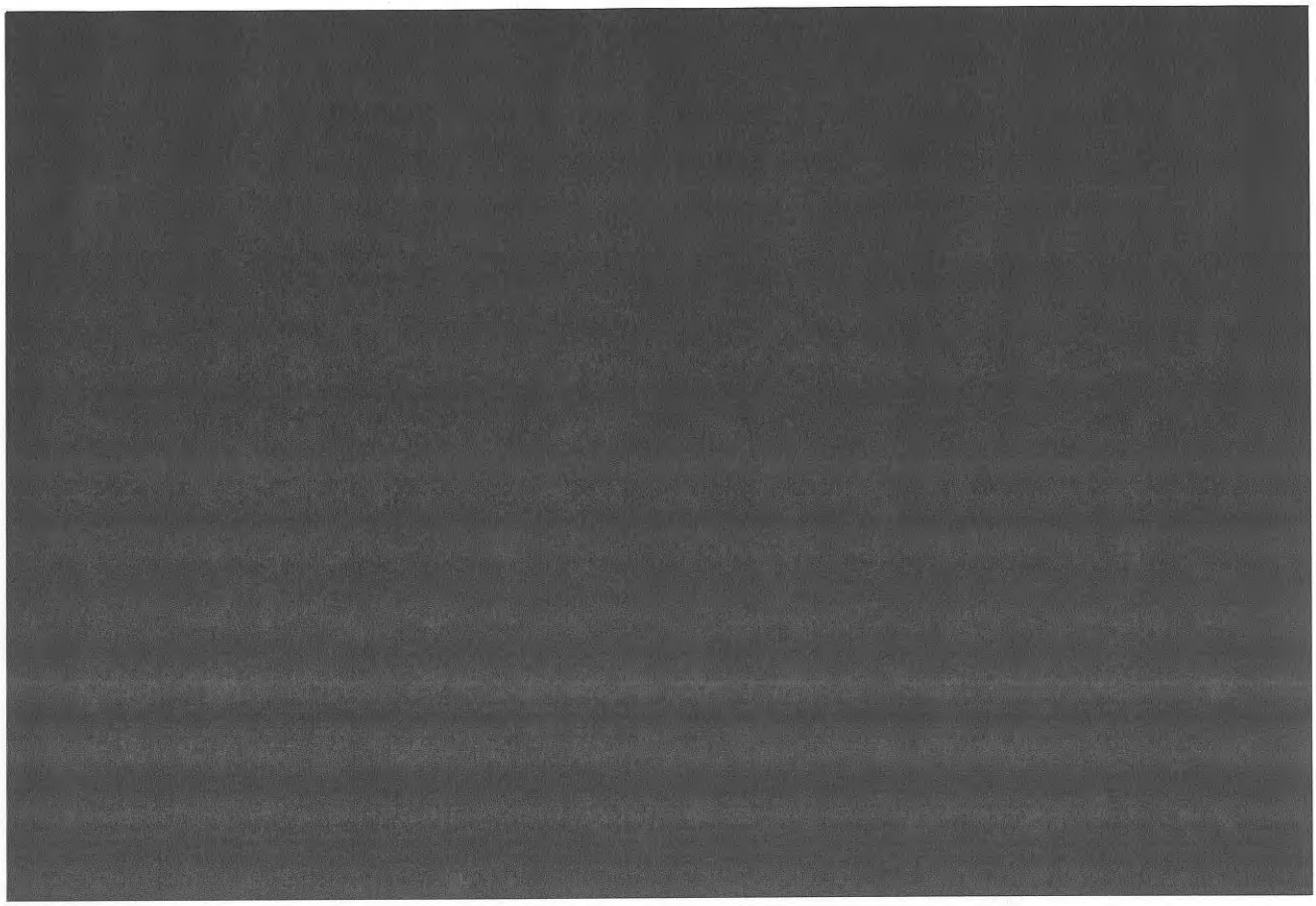


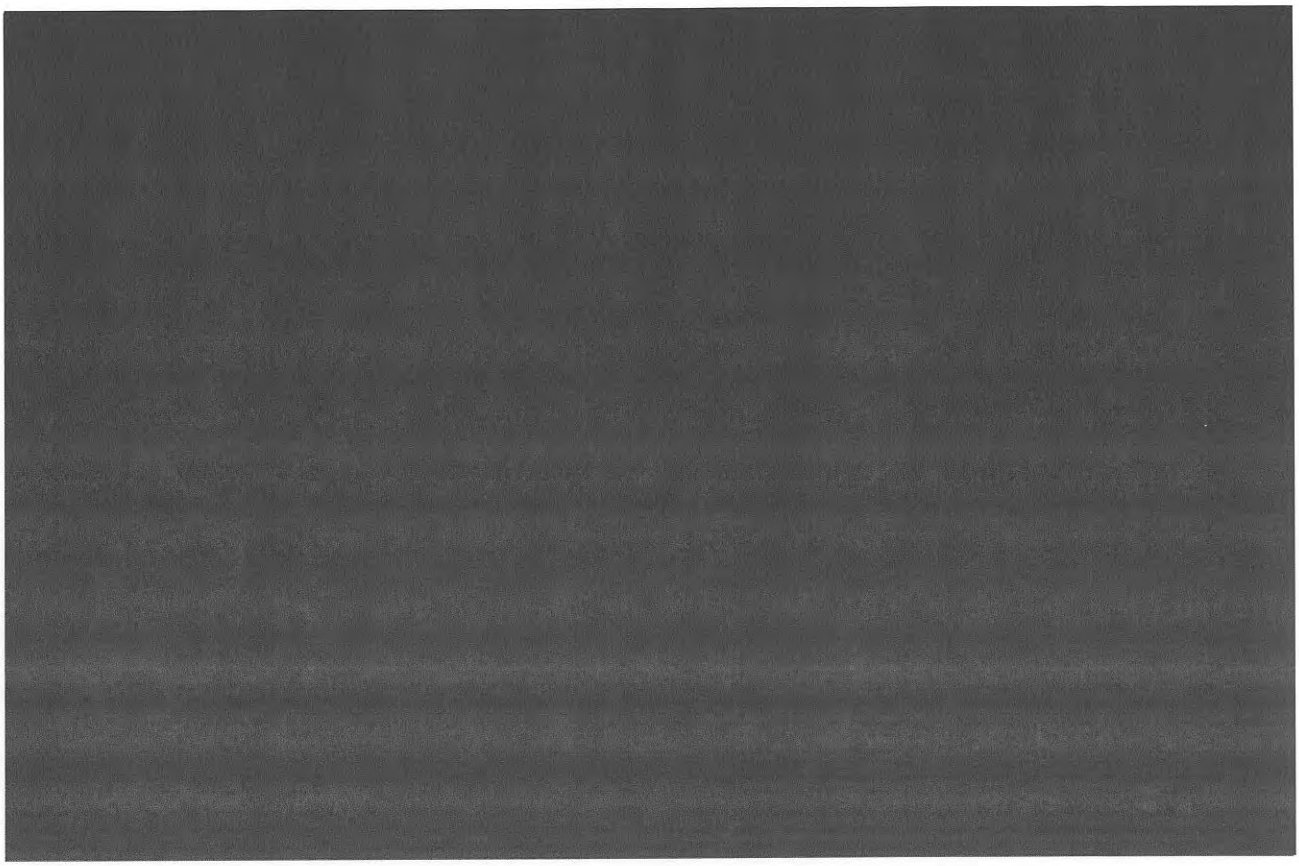




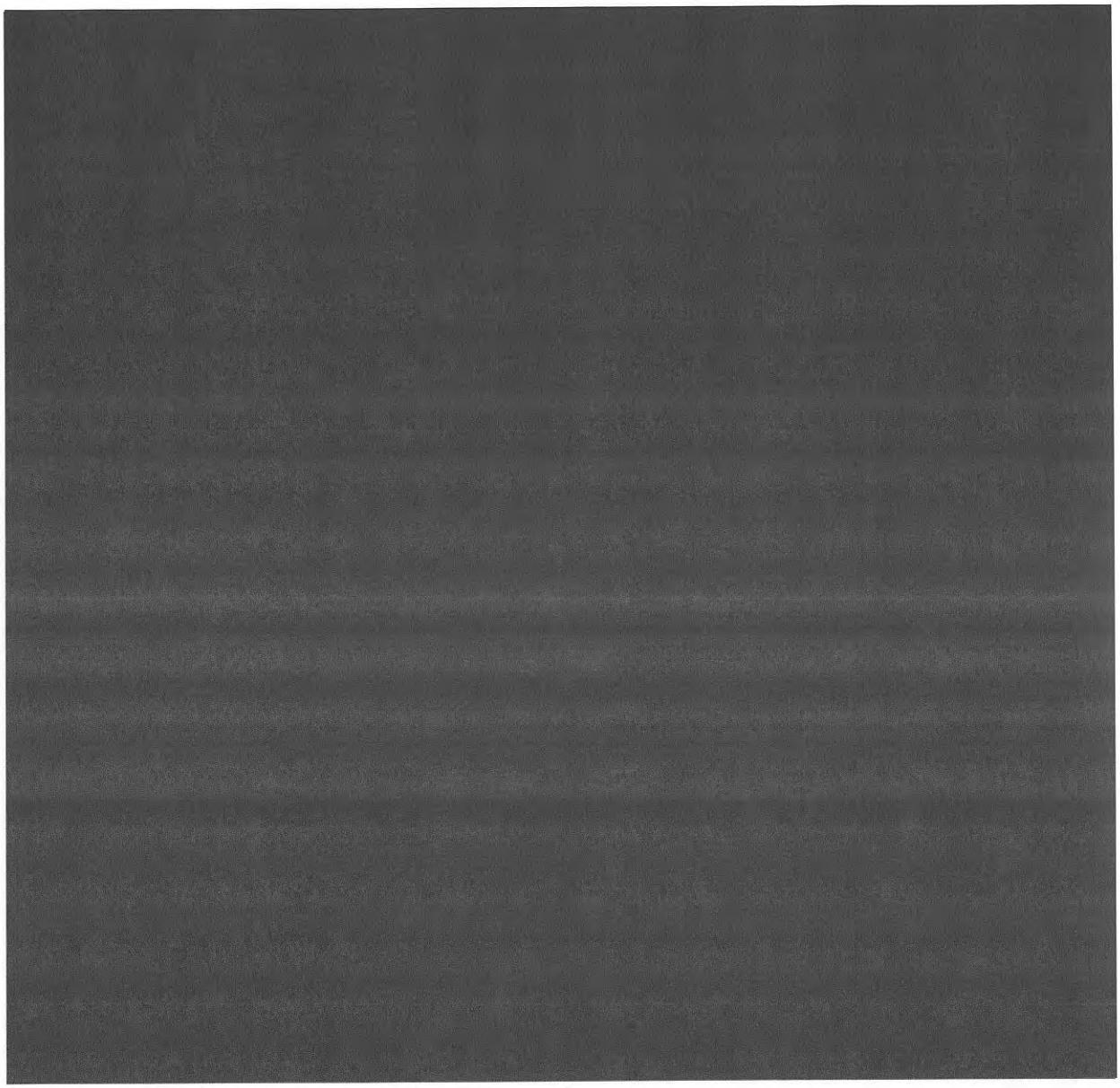


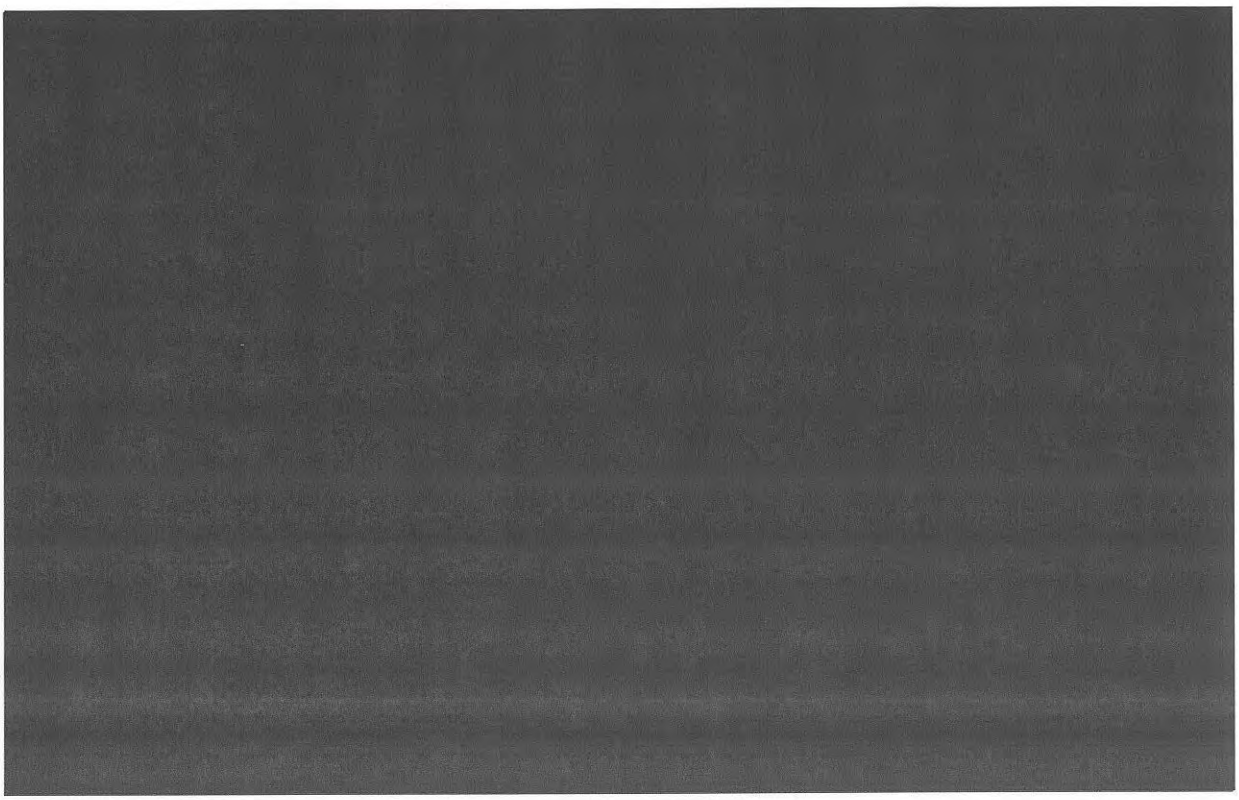


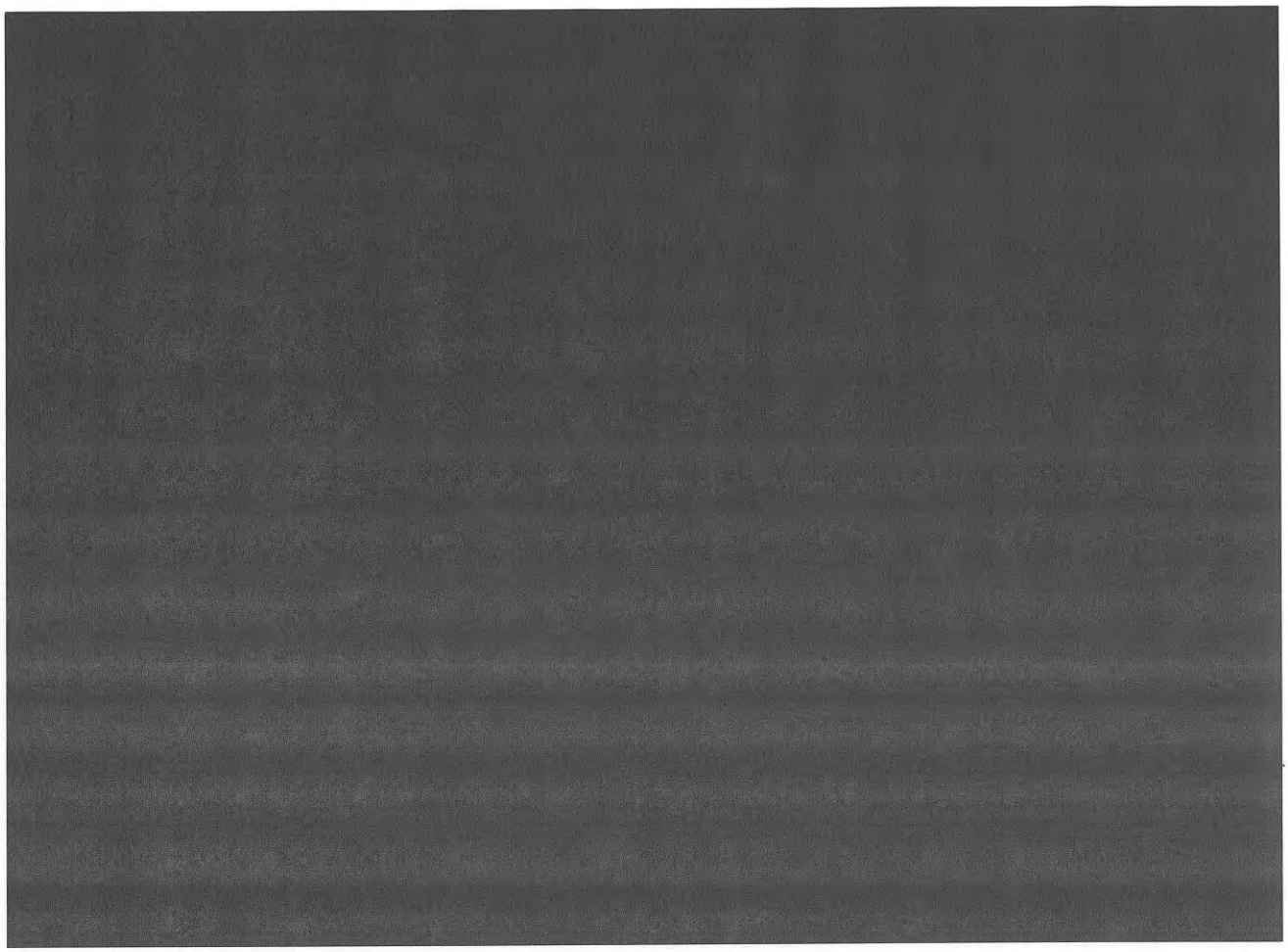


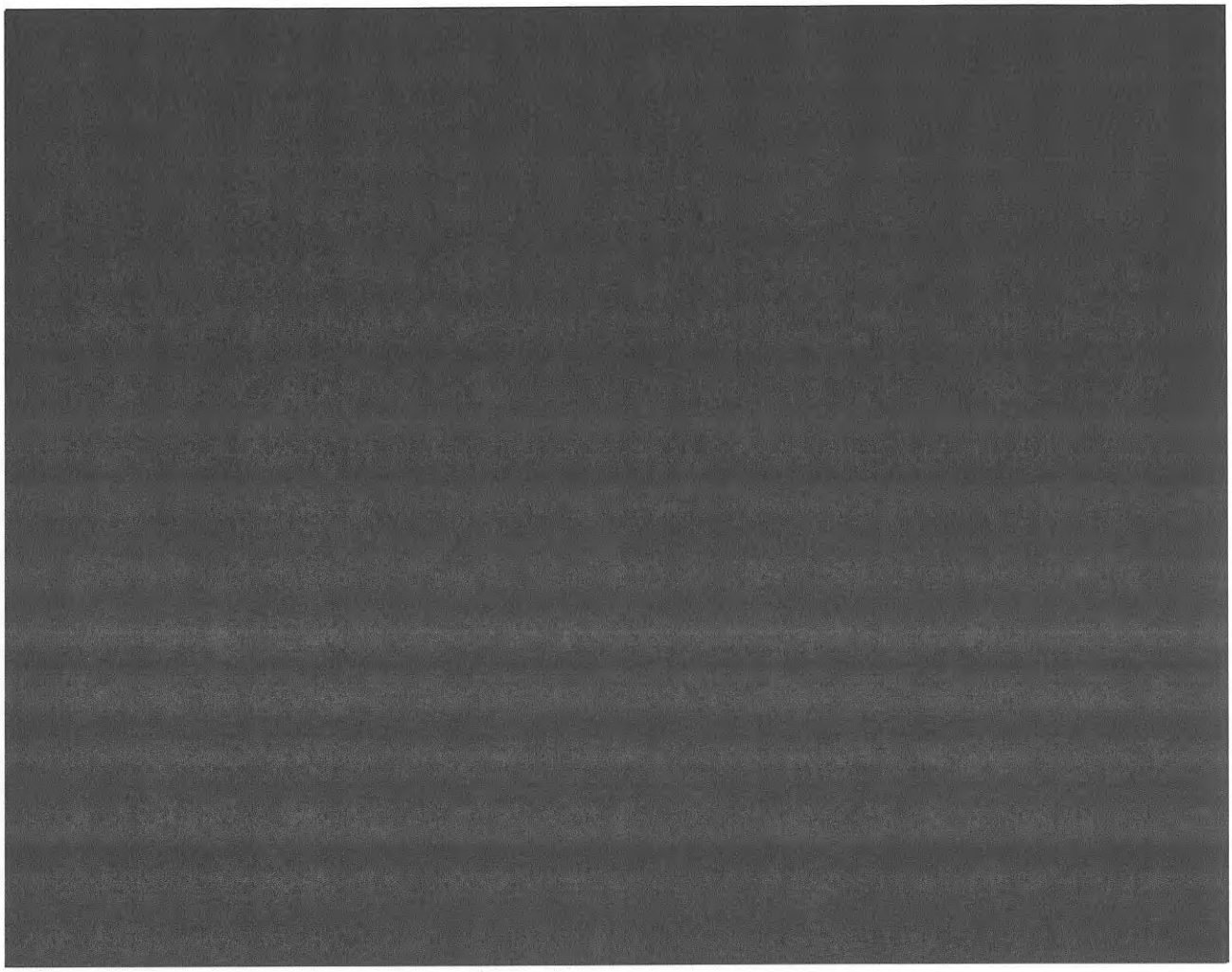


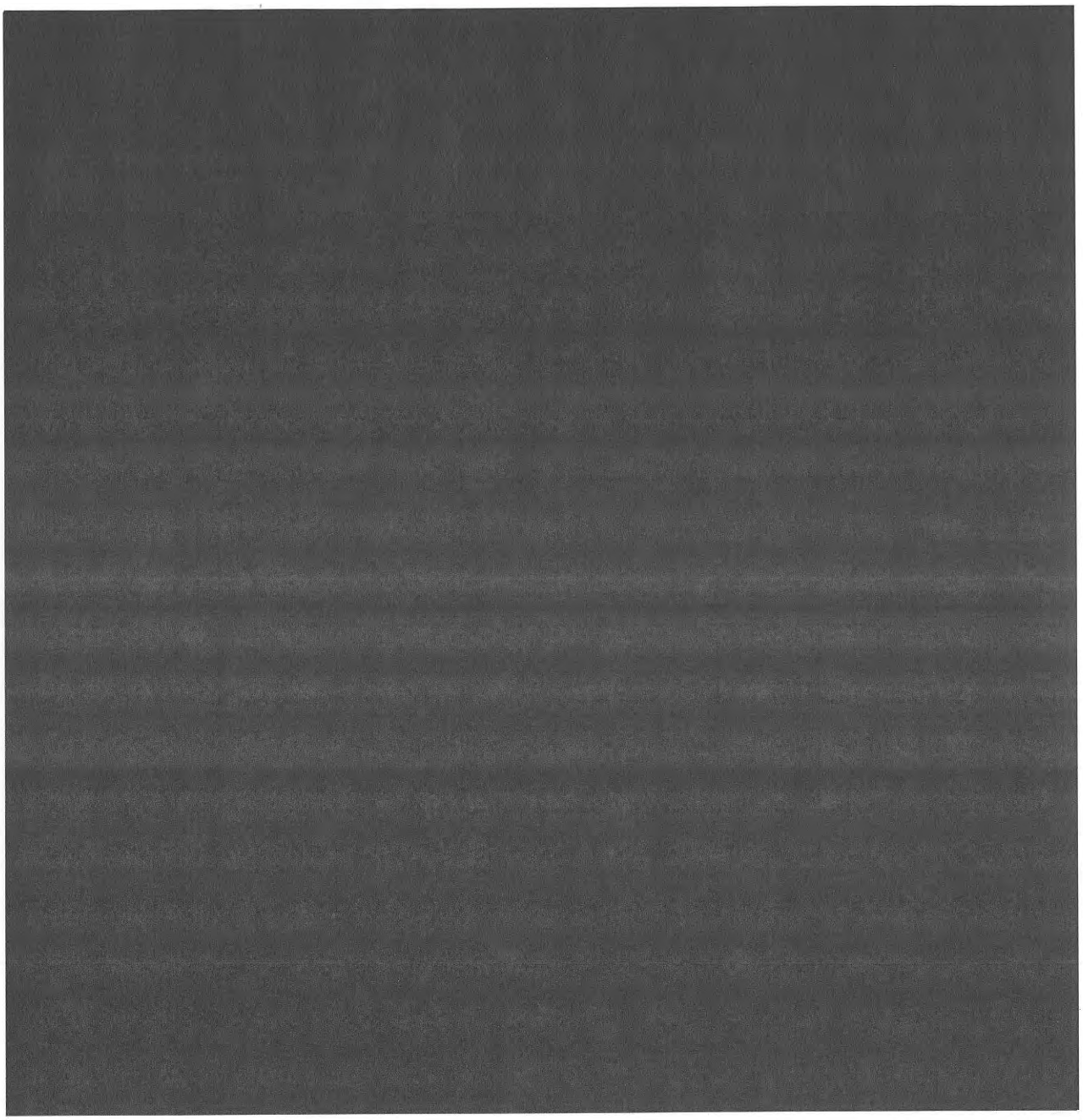
(b)(1); (b)(3); (b)(7)(A)

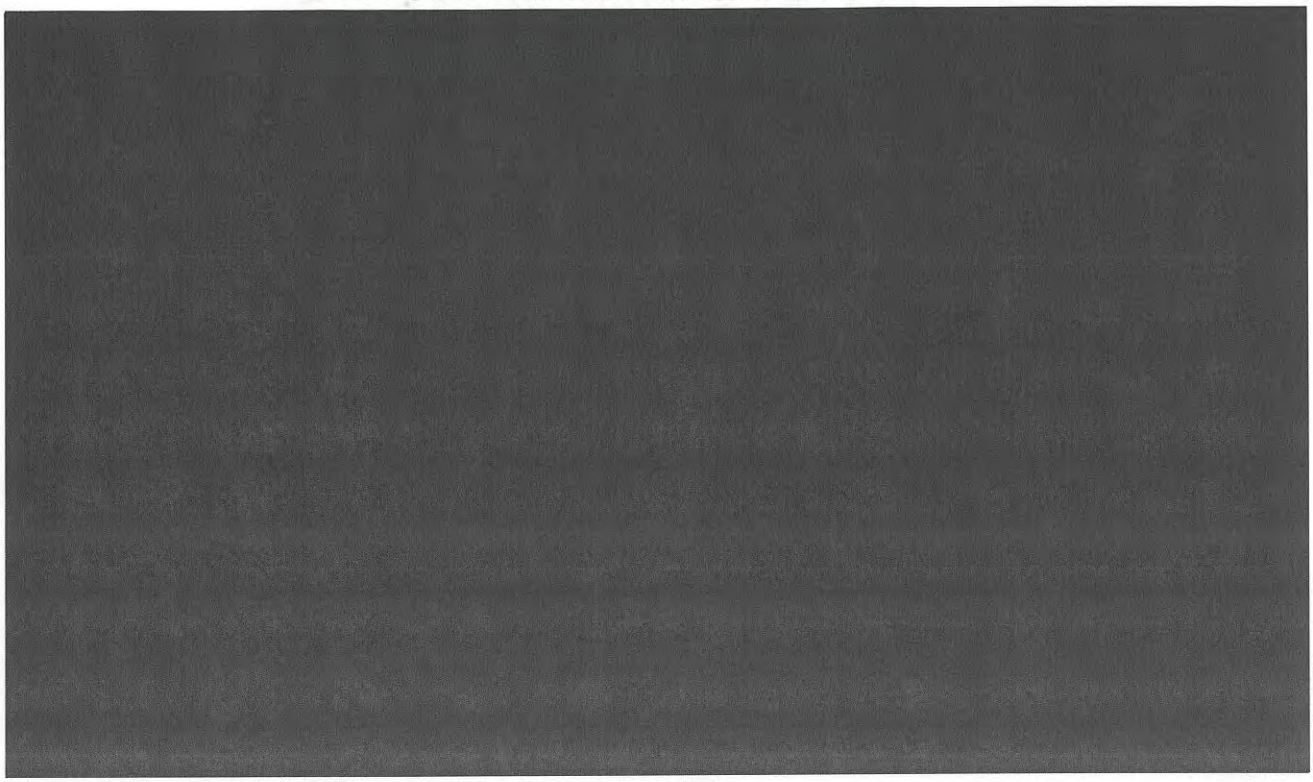




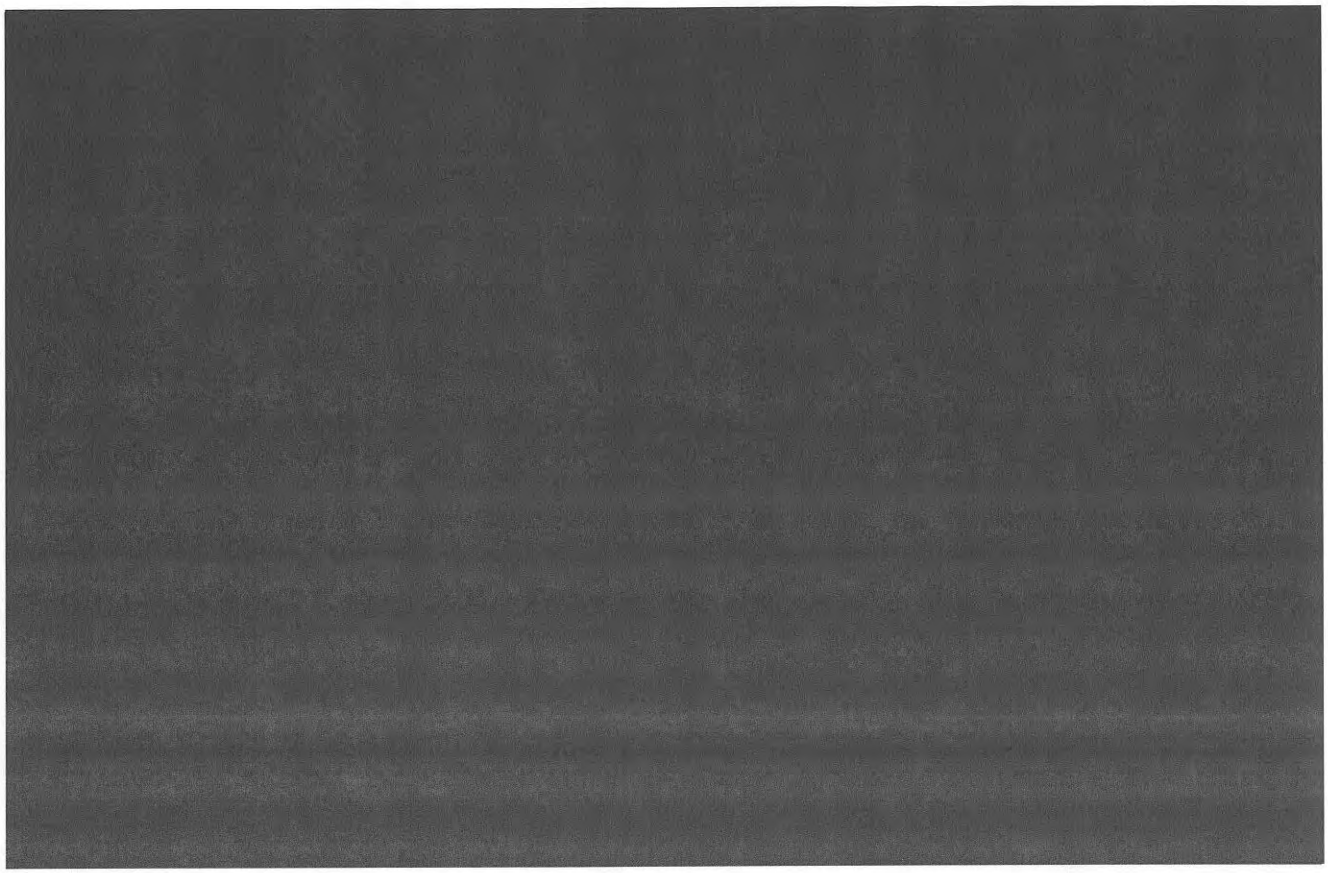


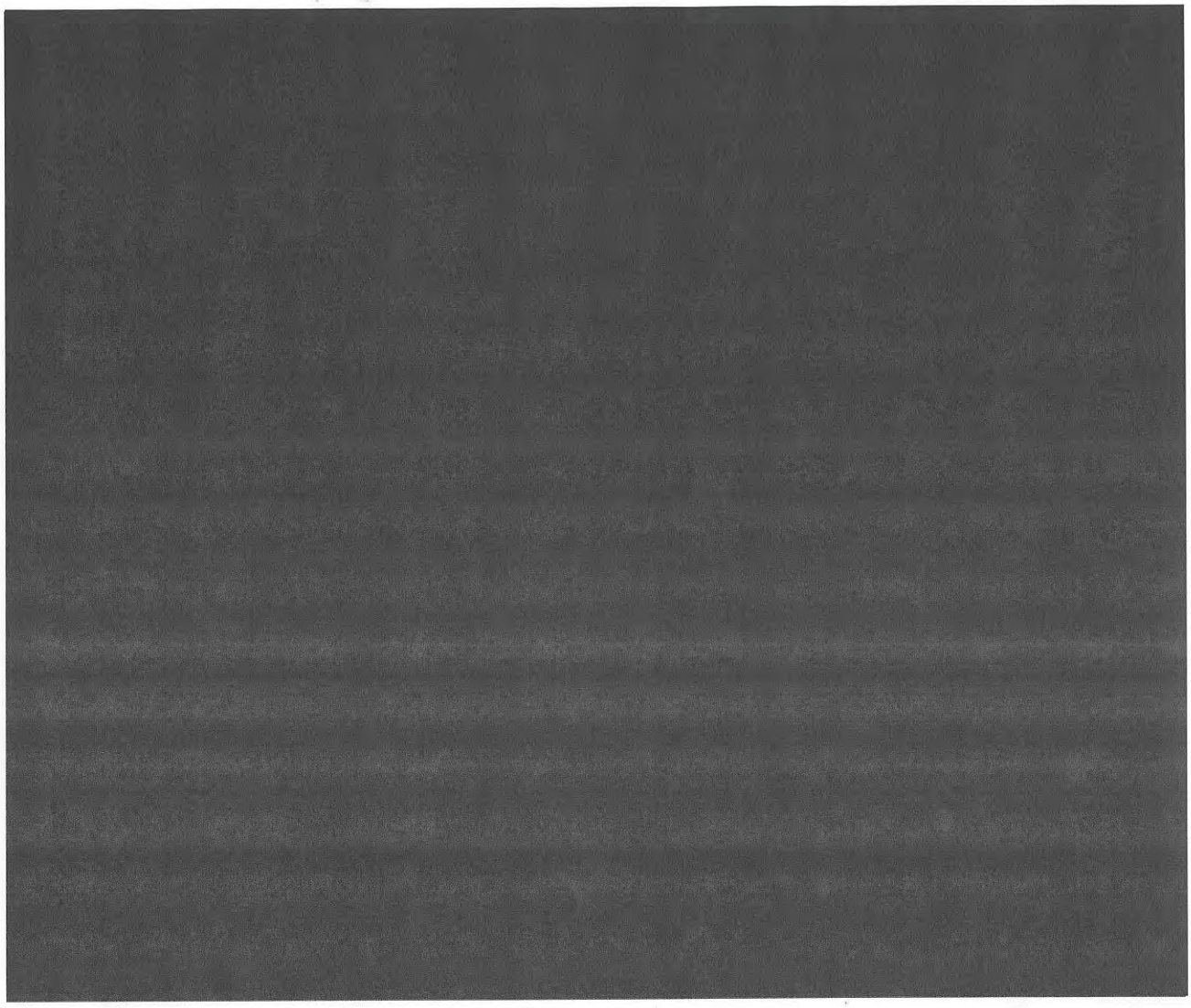


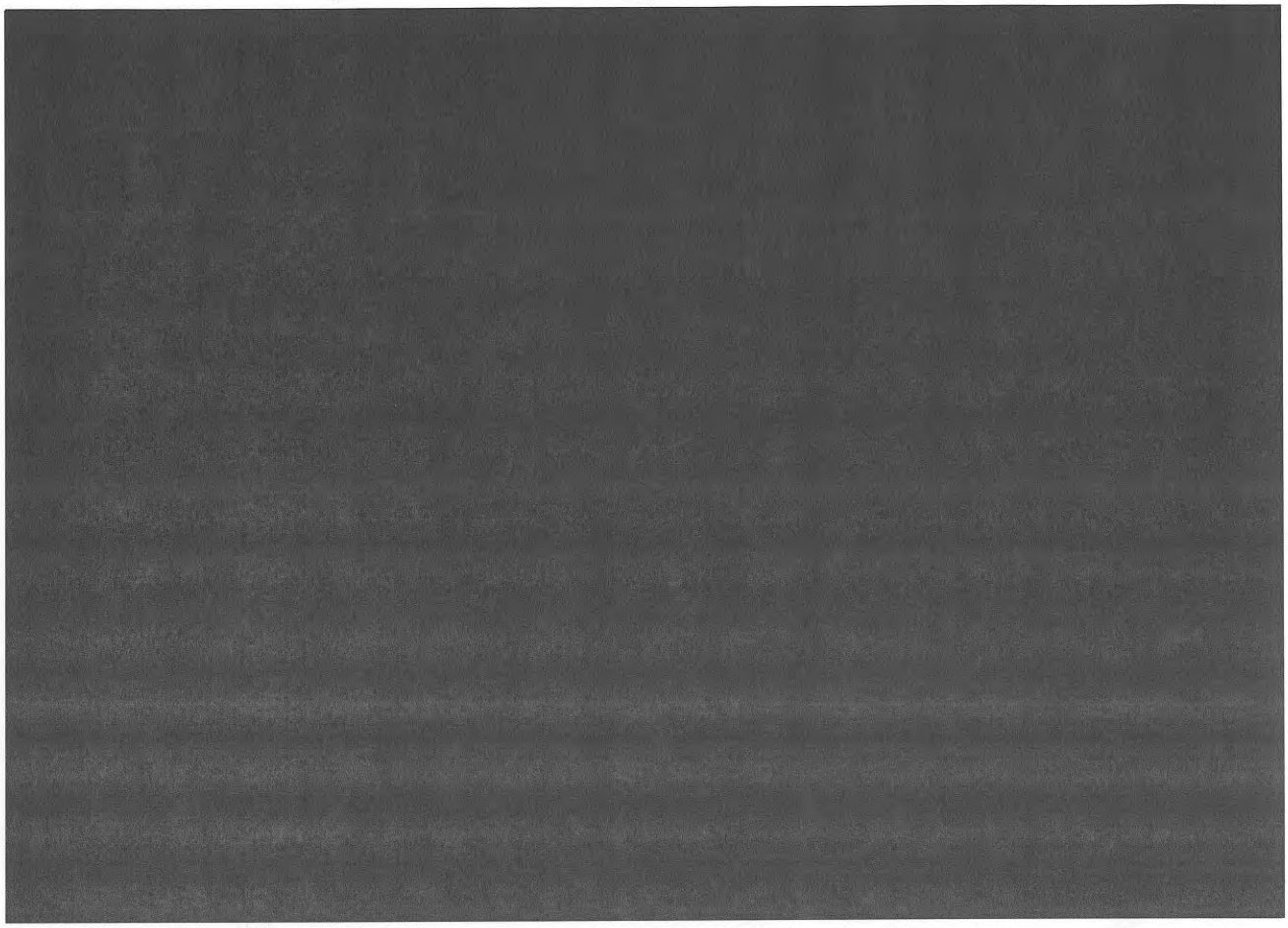


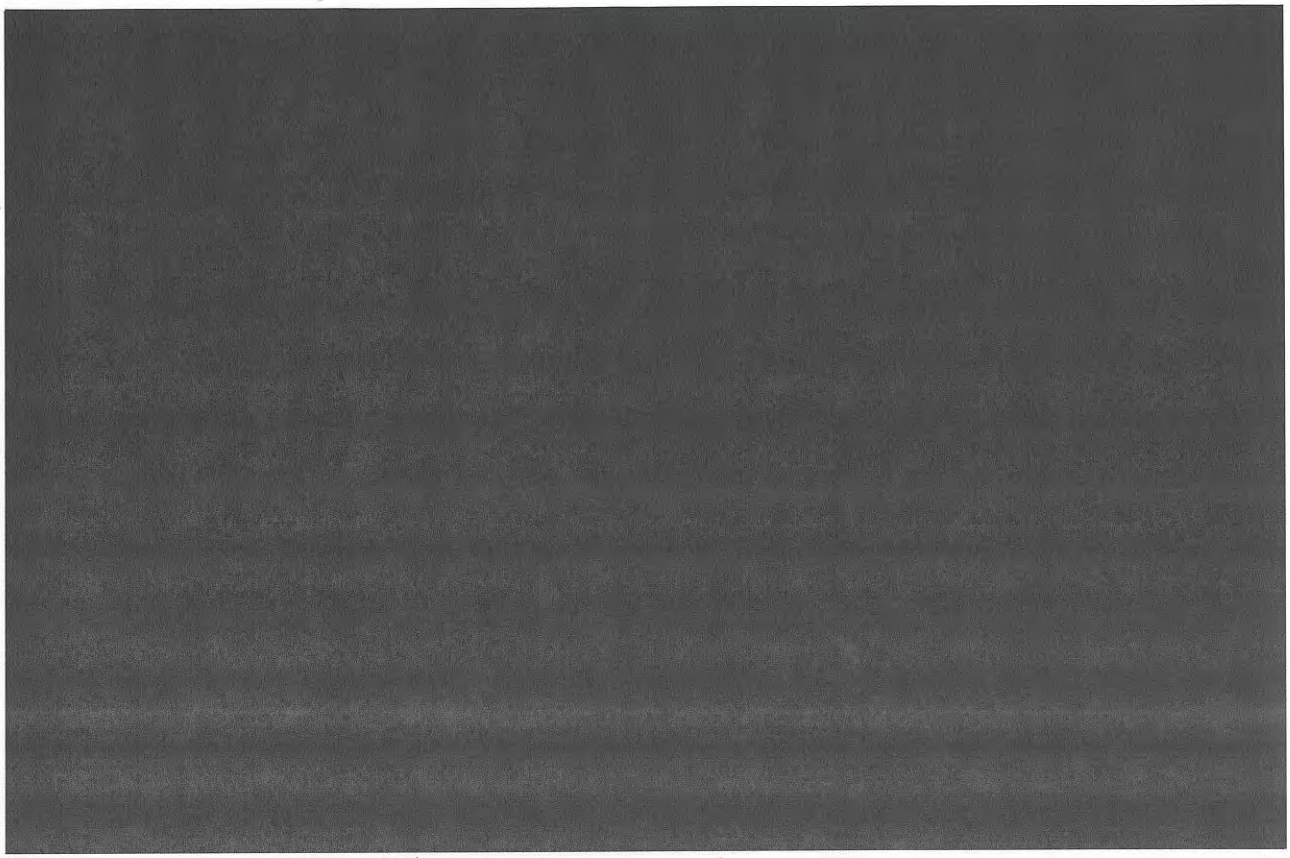


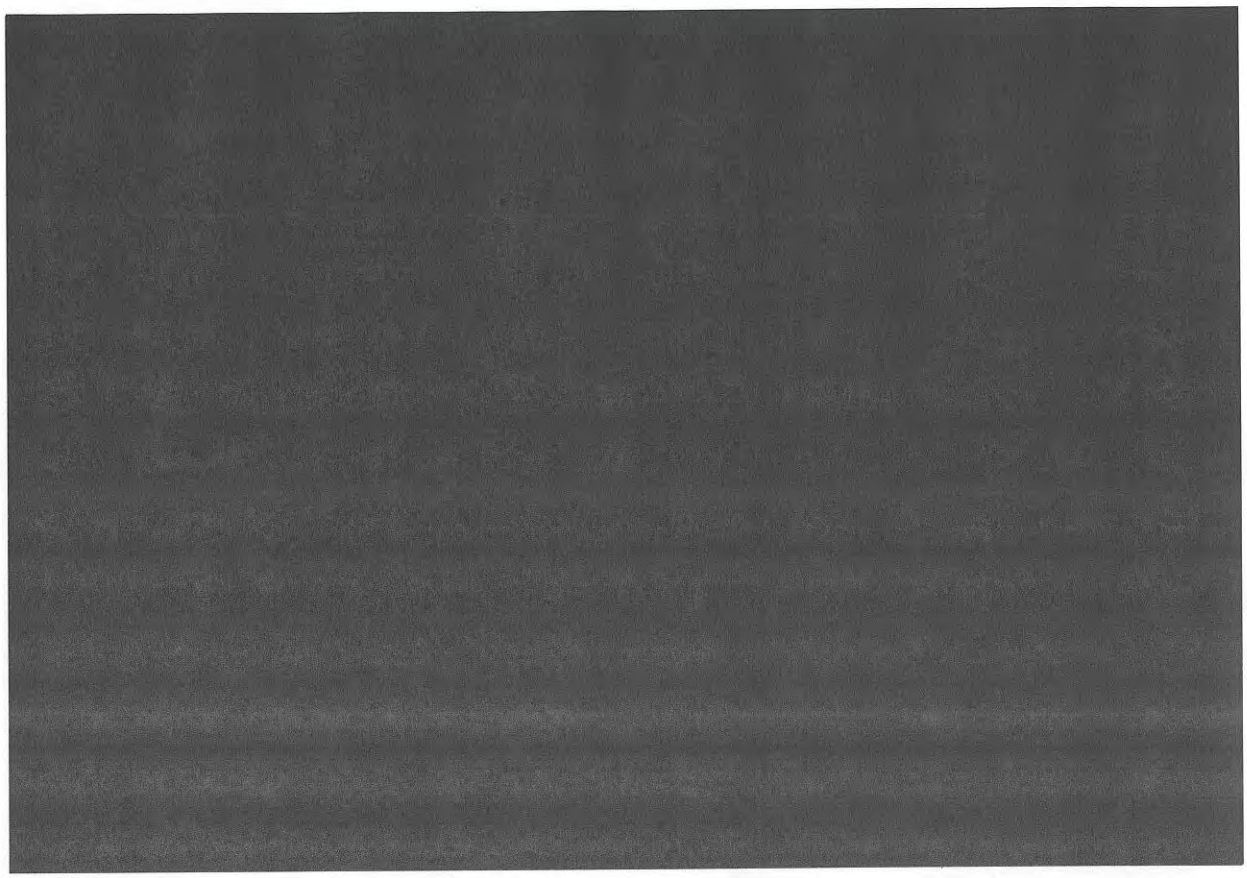
Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: 20291123

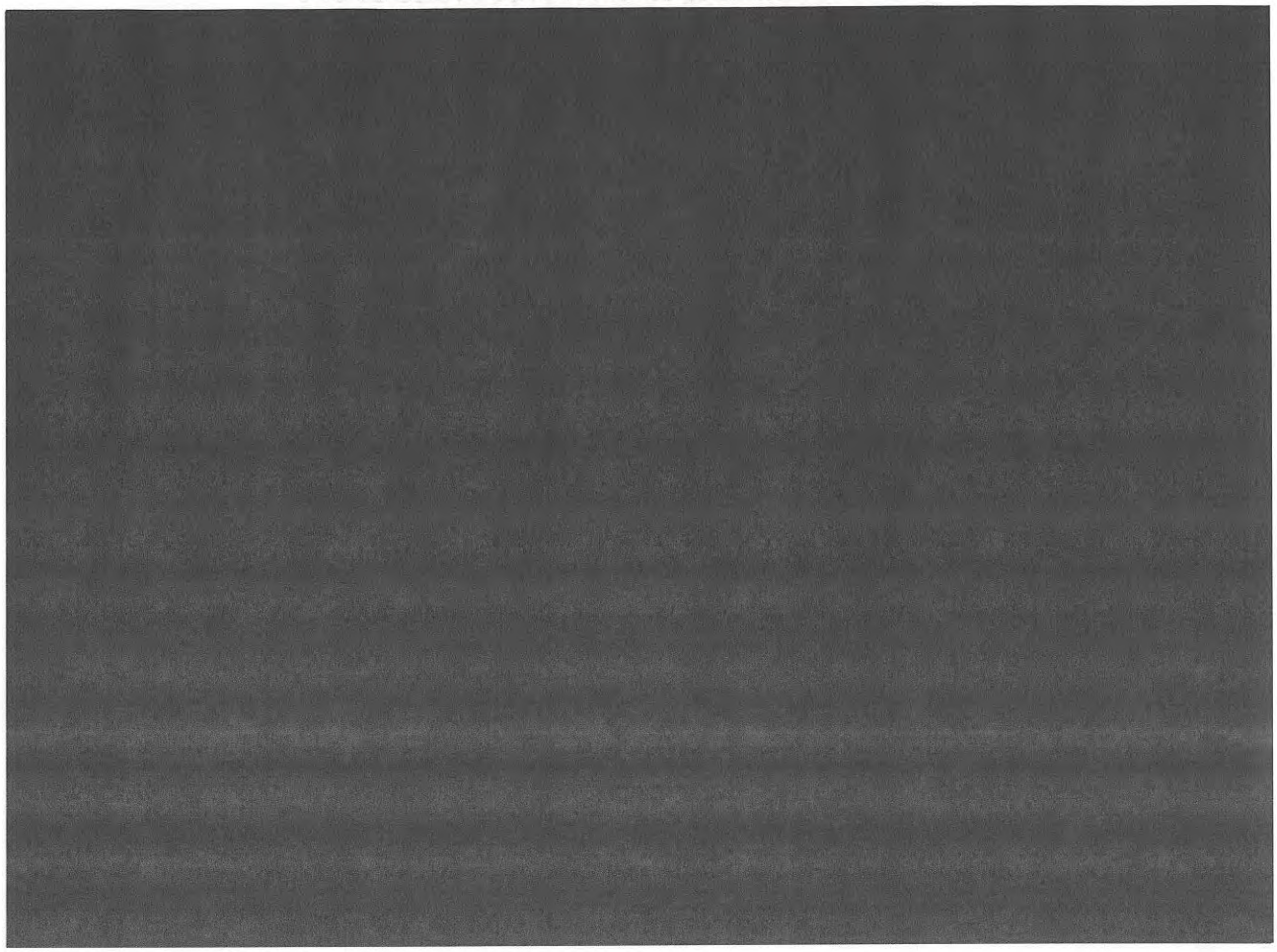


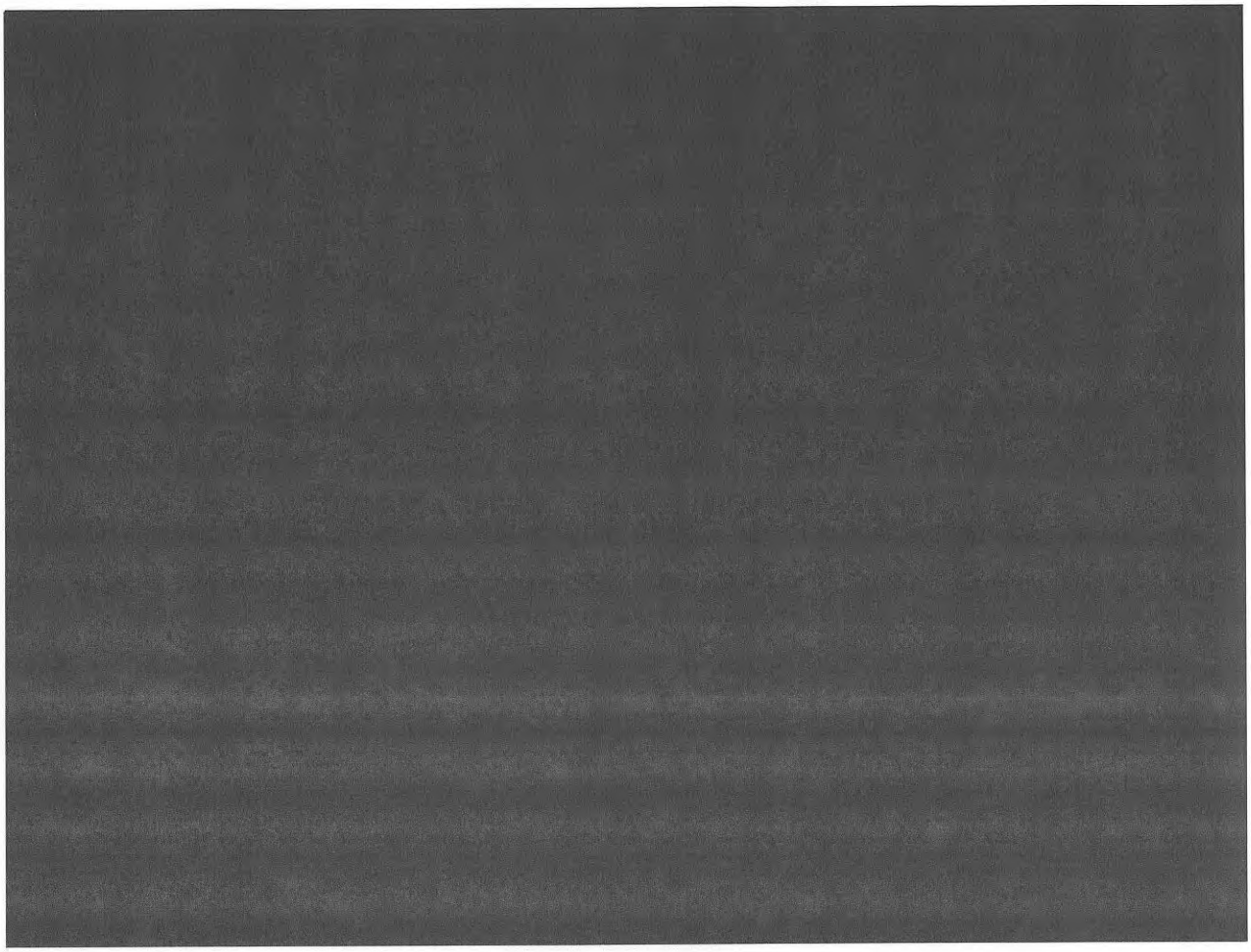




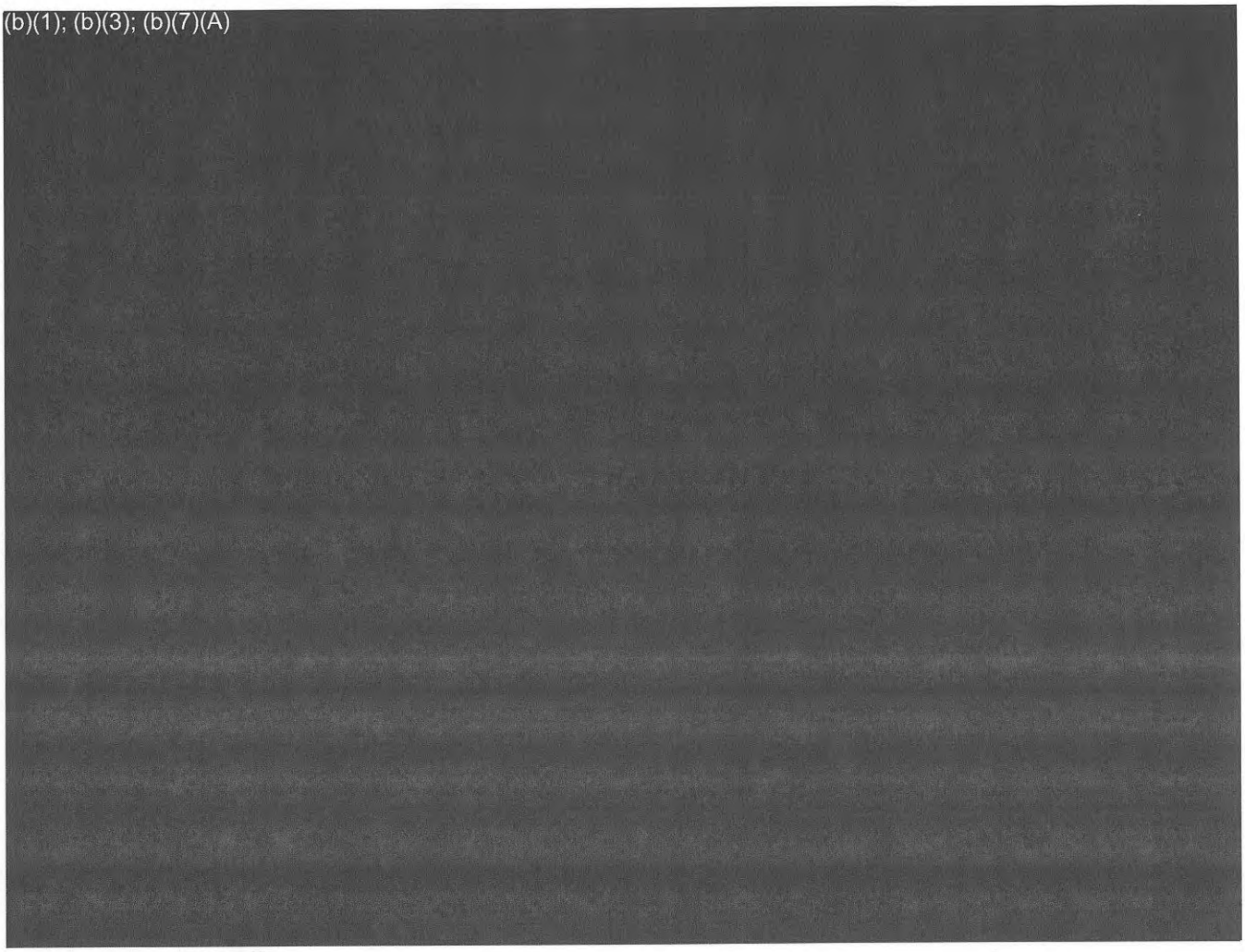


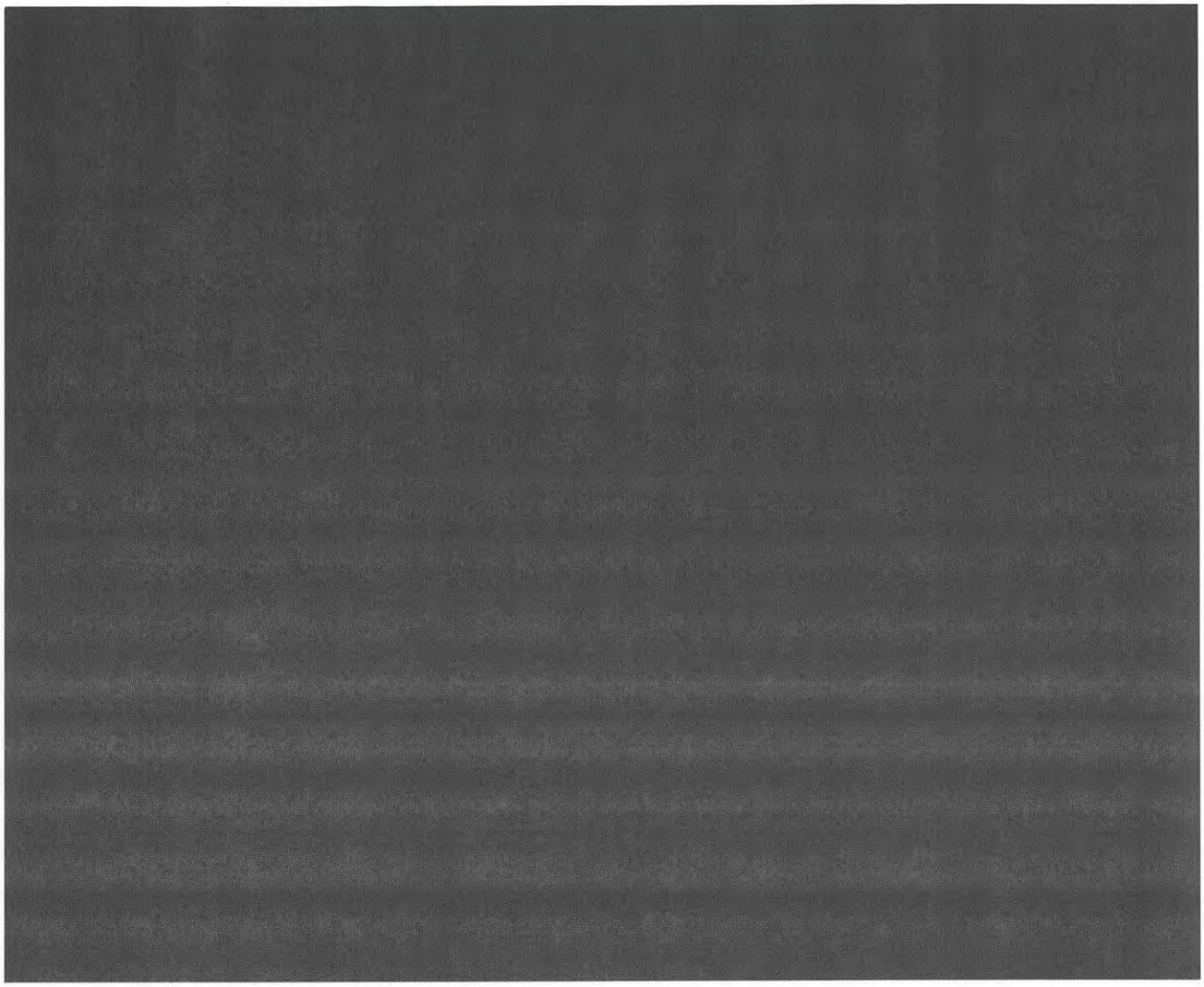


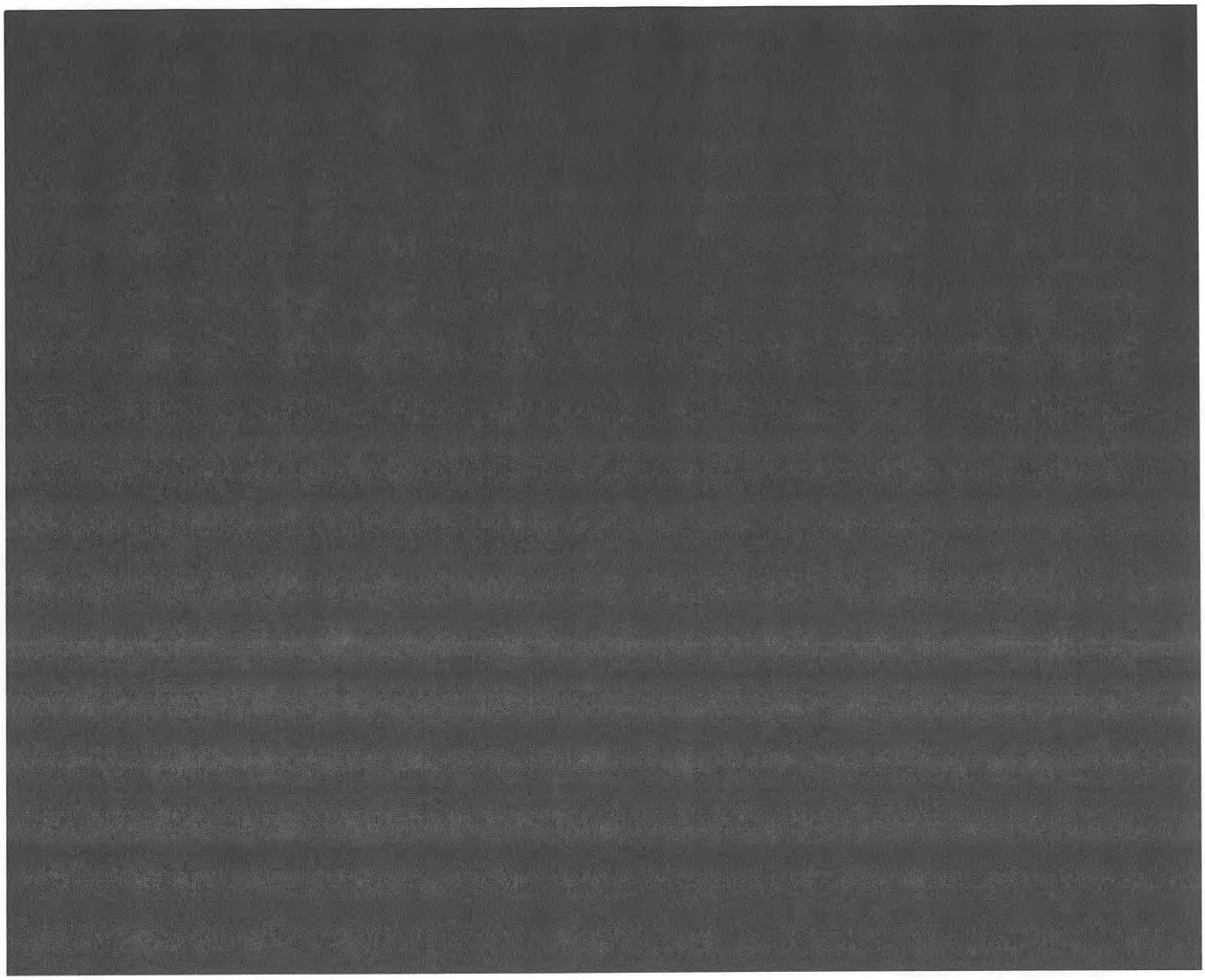


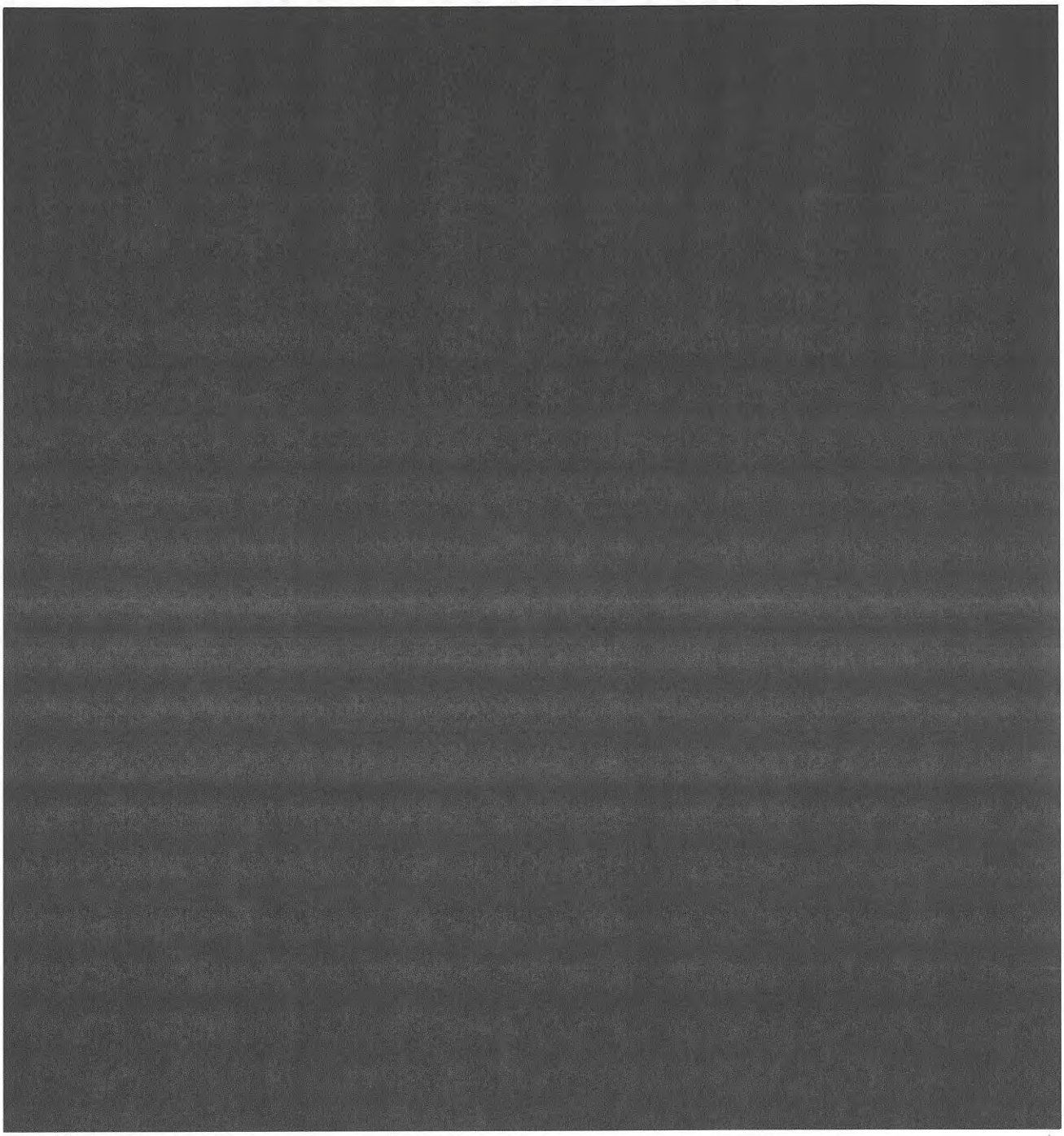


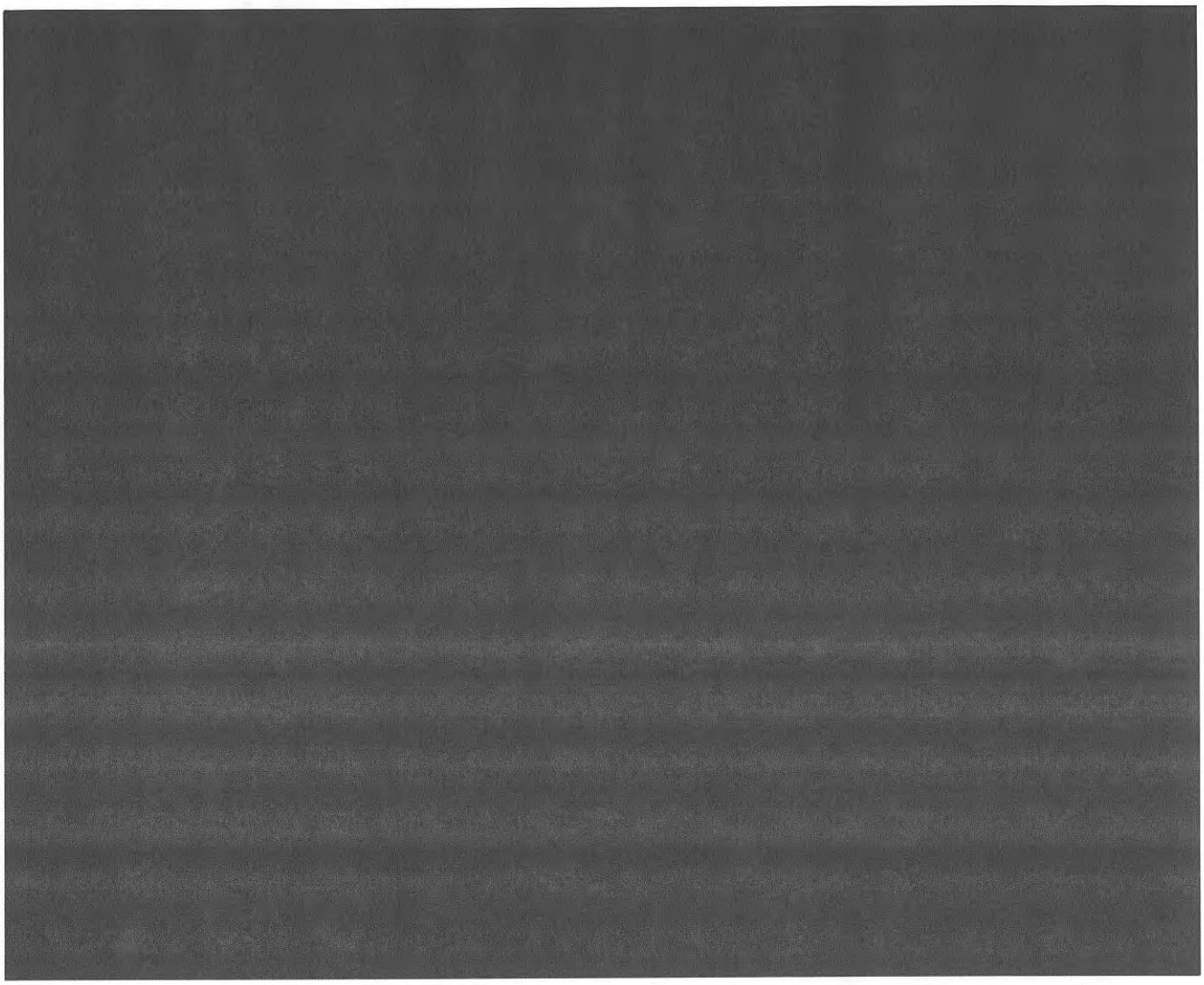
(b)(1); (b)(3); (b)(7)(A)

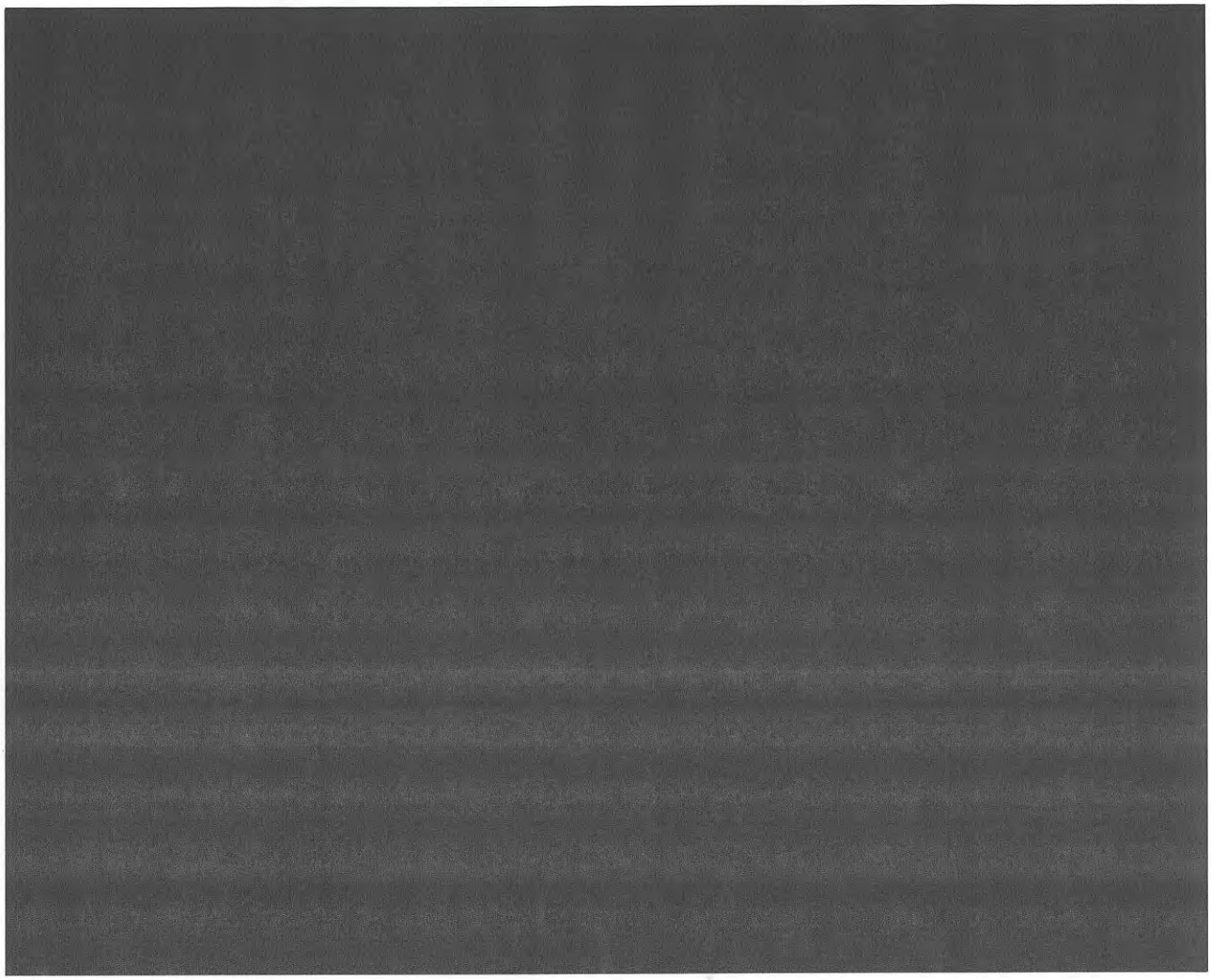












(b)(1); (b)(3); (b)(7)(A)